Product Guide
Revision B

McAfee Advanced Threat Defense 3.0.4

COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **7**

About this guide . . . 7

Audience . . . 7

Conventions . . . 7

Find product documentation . . . 8

1 Malware detection and McAfee® Advanced Threat Defense **9**

The malware threat scenario . . . 9

The McAfee Advanced Threat Defense solution . . . 10

McAfee Advanced Threat Defense deployment options . . . 12

McAfee Advanced Threat Defense advantages . . . 14

2 Setting up the McAfee Advanced Threat Defense Appliance **17**

About McAfee Advanced Threat Defense Appliance . . . 17

Functions of a McAfee Advanced Threat Defense Appliance . . . 17

Before you install the McAfee Advanced Threat Defense Appliance . . . 18

Warnings and cautions . . . 19

Usage restrictions . . . 19

Unpack the shipment . . . 20

Check your shipment . . . 20

Hardware specifications and environmental requests . . . 23

Port numbers . . . 24

Setting up McAfee Advanced Threat Defense . . . 24

Install or remove rack handles . . . 25

Install or remove the Appliance from the rack . . . 25

Turn on the McAfee Advanced Threat Defense Appliance . . . 27

Handling the front bezel . . . 27

Connect the network cable . . . 28

Configure network information for McAfee Advanced Threat Defense Appliance . . . 28

3 Accessing McAfee Advanced Threat Defense web application **31**

McAfee Advanced Threat Defense client requirements . . . 31

Access the McAfee Advanced Threat Defense web application . . . 32

4 Managing users and performance **33**

Managing McAfee Advanced Threat Defense users . . . 33

Viewing user profiles . . . 34

Add users . . . 35

Edit Users . . . 37

Delete Users . . . 38

Monitoring the McAfee Advanced Threat Defense performance . . . 38

Import McAfee Advanced Threat Defense software . . . 38

Troubleshooting . . . 39

Export McAfee Advanced Threat Defense logs . . . 40

Delete the analysis results . . . 40

5 Creating analyzer VM 41
Create a VMDK file from an ISO image . . . 42
Import a VMDK file into McAfee Advanced Threat Defense . . . 73
Convert the VMDK file to an image file . . . 74
Managing VM profiles . . . 74
View VM profiles . . . 75
Create VM profiles . . . 76
Edit VM profiles . . . 80
Delete VM profiles . . . 80
View the VM creation log . . . 81

6 Configuring McAfee Advanced Threat Defense for malware analysis 83
Terminologies . . . 83
High-level steps for configuring malware analysis . . . 86
How McAfee Advanced Threat Defense analyzes malware? . . . 87
Managing analyzer profiles . . . 87
View analyzer profiles . . . 88
Create analyzer profiles . . . 89
Edit analyzer profiles . . . 91
Delete analyzer profiles . . . 91
Integration with McAfee ePO . . . 91
Configure McAfee ePO integration . . . 92
Specify proxy server for internet connectivity . . . 93
Configure the proxy DNS settings . . . 94

7 Analyzing malware 97
Upload files for analysis using McAfee Advanced Threat Defense web application . . . 97
Upload files for analysis in user-interactive mode . . . 98
Upload files for analysis using SFTP . . . 100
Monitor the status of malware analysis . . . 100
View the analysis results . . . 102
View the Analysis Summary report . . . 104
Dropped files report . . . 110
Disassembly Results . . . 110
Logic Path Graph . . . 111
User API Log . . . 116
Download the complete results .zip file . . . 116
Working with the McAfee Advanced Threat Defense Dashboard . . . 117
Malware analysis monitors . . . 118
VM Creation Status monitor . . . 121
McAfee Advanced Threat Defense performance monitors . . . 121

8 CLI commands for McAfee Advanced Threat Defense 123
Issue of CLI commands . . . 123
How to issue a command through the console . . . 123
Issuing a command through SSH . . . 123
Logging on to the McAfee Advanced Threat Defense Appliance using an SSH client . . . 124
Auto-complete . . . 124
CLI syntax . . . 124
Mandatory commands . . . 124
Log on to the CLI . . . 125
Meaning of "?" . . . 125
Managing the disks of McAfee Advanced Threat Defense Appliance . . . 125
List of CLI commands . . . 126
Blacklist . . . 126
clearstats . . . 127

createDefaultVms . . . 127
deleteblacklist . . . 127
deletesamplereport . . . 127
diskcleanup . . . 128
Exit . . . 128
factorydefaults . . . 128
gti_restart . . . 128
help . . . 128
list . . . 129
nslookup . . . 129
passwd . . . 129
ping . . . 129
quit . . . 129
reboot . . . 129
resetusertimeout . . . 130
route add/delete network . . . 130
set appliance ip . . . 130
set appliance gateway . . . 131
set appliance name . . . 131
set intfport . . . 131
set intfport auto . . . 131
set intfport ip . . . 132
set intfport speed duplex . . . 132
set mgmtport auto . . . 132
set mgmtport speed and duplex . . . 132
set_ui_timeout . . . 133
setwhitelist . . . 133
show . . . 133
show epo-stats nsp . . . 134
show history . . . 134
show intfport . . . 134
show nsp scandetails . . . 134
show route . . . 135
shutdown . . . 136
status . . . 136
update_avdat . . . 136
watchdog . . . 136
whitelist . . . 137

Index **139**

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- Administrators — People who implement and enforce the company's security program.
- Users — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Malware detection and McAfee® Advanced Threat Defense

Over the years, malware has evolved into a sophisticated tool for malicious activities such as stealing valuable information, accessing your computer resources without your knowledge, and for disrupting business operations. At the same time, technological advancement provides limitless options to deliver malicious files to unsuspecting users. Hundreds of thousands of new malware variants every day make the job of malware detection even more complex. Traditional anti-malware techniques are no longer sufficient to protect your network.

McAfee's response to this challenge is the McAfee Advanced Threat Defense solution. This is an on-premise Appliance that facilitates detection and prevention of malware. McAfee Advanced Threat Defense provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.

McAfee Advanced Threat Defense has the added advantage of being an integrated solution. In addition to its own multi-level threat detection capabilities, its ability to seamlessly integrate with other McAfee security products, protects your network against malware and other Advanced Persistent Threats (APTs).

Contents

- *The malware threat scenario*
- *The McAfee Advanced Threat Defense solution*

The malware threat scenario

Any software capable of being involved in hostile activities with respect to a computer, application, or network can be termed as malware. McAfee Advanced Threat Defense is designed for detecting file-based malware.

Earlier, users received malware as attachments in their emails. With the upsurge in Internet applications, users only need to click a link to download files. Today, there are many other options to post such files — blogs, social networking sites, web sites, chat messages, web mails, message boards, and so on. The key challenges in tackling this issue are to detect malware in the shortest possible time and also contain it from spreading to other computers.

There are four major aspects to an anti-malware strategy:

- Detection of file downloads: When a user attempts to download a file from an external resource, your security product must be able to detect it.
- Analysis of the file for malware: You must be able to verify if the file contains any known malware.

- Block future downloads of the same file: Subsequently, if the file is found to be malicious, your anti-malware protection must prevent future downloads of the same file or its variants.
- Identify and remediate affected hosts: Your security system must be able to identify the host which executed the malware, and also detect the hosts to which it has spread. Then, it must provide an option to quarantine the affected hosts until they are clean again.

The McAfee Advanced Threat Defense solution

A security solution that relies on a single method or process might not be adequate to provide complete and reliable protection from malware attacks. You might need a multi-layered solution that involves various techniques and products. The solution can include pattern matching, global reputation, program emulation, static analysis, and dynamic analysis. All these layers must be seamlessly integrated and provide you with a single point of control for easy configuration and management. For example, pattern matching might not detect zero-day attacks. Similarly, static analysis takes less time than dynamic analysis. However, malware can avoid static analysis by code obfuscation. Malware can escape dynamic analysis too by delaying execution or take an alternate execution path if the malware detects that it is being run in a sandbox environment. This is why a reliable protection from malware requires a multi-level approach.

There are other industry-leading McAfee anti-malware products for the web, network, and endpoints. However, McAfee recognizes that a robust anti-malware solution requires a multi-layered approach, the result of which is McAfee Advanced Threat Defense.

The McAfee Advanced Threat Defense solution primarily consists of the McAfee Advanced Threat Defense Appliance and the pre-installed software. The McAfee Advanced Threat Defense Appliance is available in two models. The standard model is the ATD-3000. The high-end model is the ATD-6000.

McAfee Advanced Threat Defense integrates its native capabilities with other McAfee products to provide you a multilayered defense mechanism against malware:

- Its preliminary detection mechanism consists of a local blacklist to quickly detect known malware.
- It integrates with McAfee® Global Threat Intelligence™ (McAfee GTI) for cloud-lookups to detect malware that has already been identified by organizations throughout the globe.
- It has the McAfee Gateway Anti-Malware Engine embedded within it for emulation capability.

- It has the McAfee Anti-Malware Engine embedded within it for signature-based detection.
- It dynamically analyzes the file by executing it in a virtual sandbox environment. Based on how the file behaves, McAfee Advanced Threat Defense determines its malicious nature.

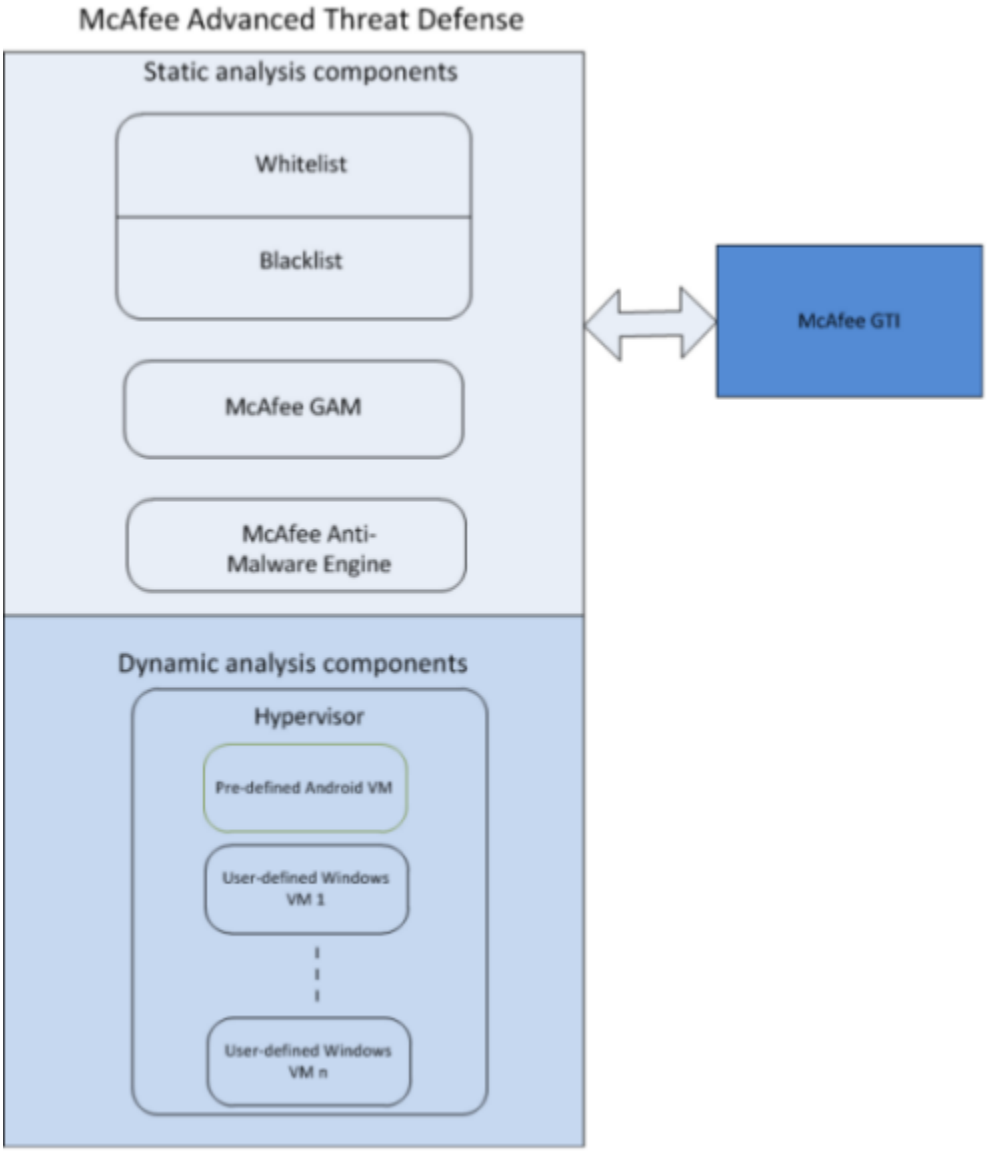


Figure 1-1 Components for malware analysis

McAfee Advanced Threat Defense deployment options

You can deploy McAfee Advanced Threat Defense in the following ways:

- Standalone deployment — This is a simple way of deploying McAfee Advanced Threat Defense. In this case, it is not integrated with other externally installed McAfee products. When deployed as a standalone Appliance, you can manually submit the suspicious files using the McAfee Advanced Threat Defense web application. Alternatively, you can submit the samples using an FTP client. This deployment option is used, for example, during the testing and evaluation phase, to fine-tune configuration, and to analyze suspicious files in an isolated network segment.

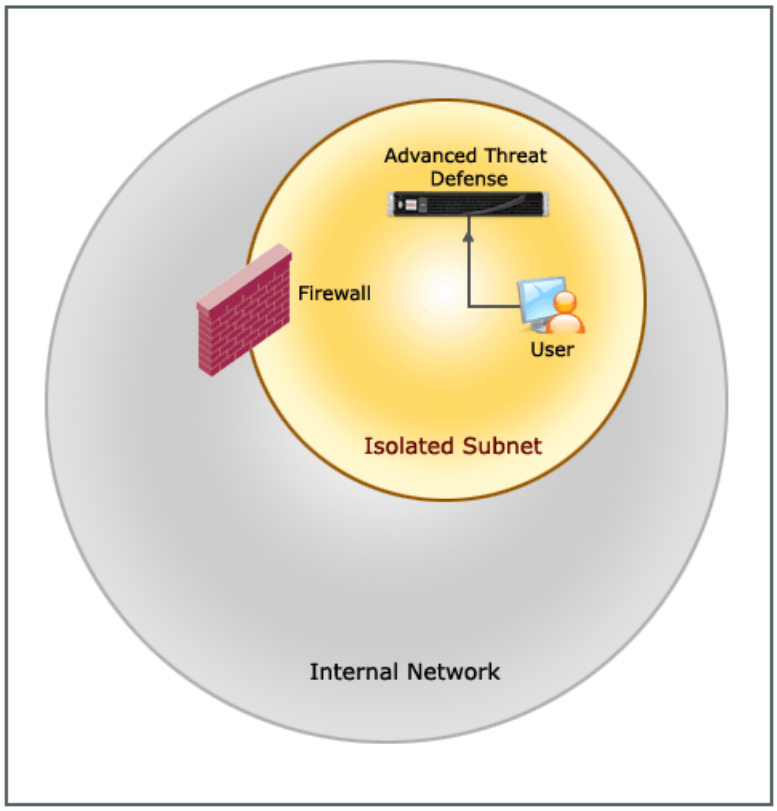


Figure 1-2 A standalone deployment scenario

- Integration with Network Security Platform — This deployment involves integrating McAfee Advanced Threat Defense with Network Security Platform Sensor and Manager.

  Based on how you have configured the corresponding Advanced Malware policy, an inline Sensor detects a file download and sends a copy of the file to McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense detects a malware within a few seconds, the Sensor can block the download. The Manager displays the results of the analysis from McAfee Advanced Threat Defense.

  If McAfee Advanced Threat Defense requires more time for analysis, the Sensor allows the file to be downloaded. If McAfee Advanced Threat Defense detects a malware after the file has been downloaded, it informs Network Security Platform, and you can use the Sensor to quarantine the host until it is cleaned and remediated. You can configure the Manager to update all the Sensors about this malicious file. Therefore, if that file is downloaded again anywhere in your network, your Sensors might be able to block it.

  For information on how to integrate Network Security Platform and McAfee Advanced Threat Defense, refer to the latest *Network Security Platform Integration Guide.*

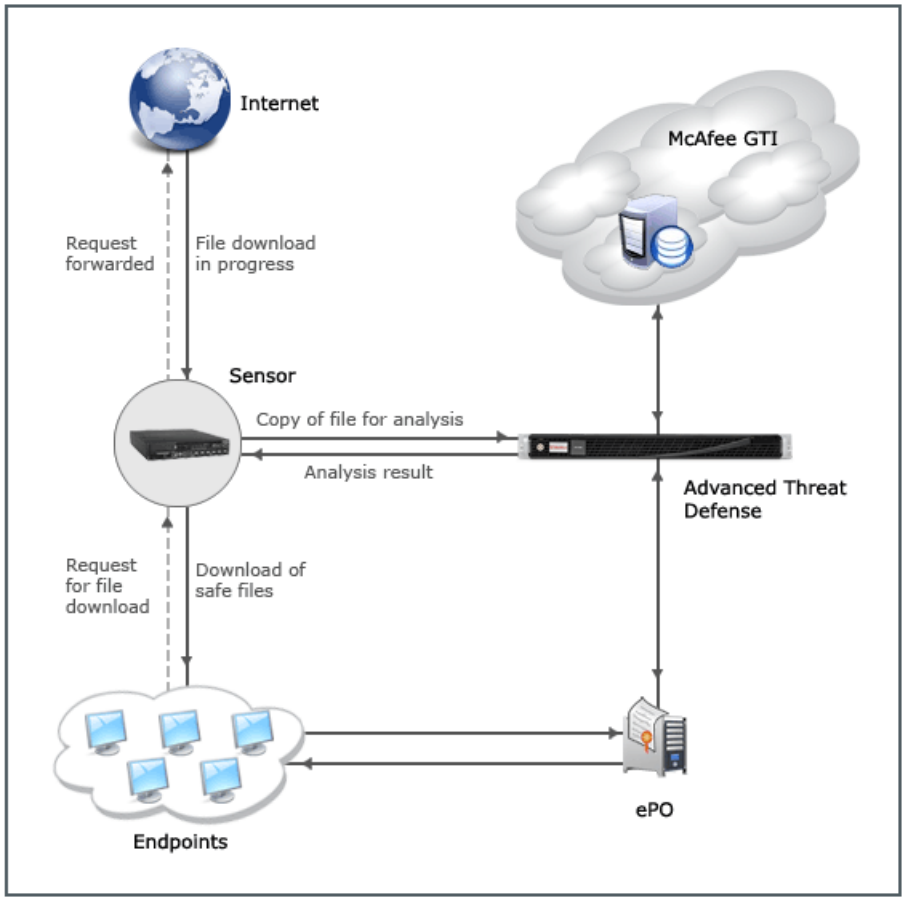


Figure 1-3 Integration with Network Security Platform and McAfee ePO

- Integration with McAfee® Web Gateway — You can configure McAfee Advanced Threat Defense as an additional engine for anti-malware protection. When your network user downloads a file, the native McAfee Gateway Anti-malware Engine on McAfee® Web Gateway scans the file and determines a malware score. Based on this score and the file type, McAfee® Web Gateway sends a copy of the file to McAfee Advanced Threat Defense for deeper inspection and dynamic analysis. A progress page informs your users that the requested file is being analyzed for malware. Based on the malware severity level reported by McAfee Advanced Threat Defense, McAfee® Web Gateway determines if the file is allowed or blocked. If it is blocked, the reasons are displayed for your users. You can view the details of the malware that was detected in the log file.

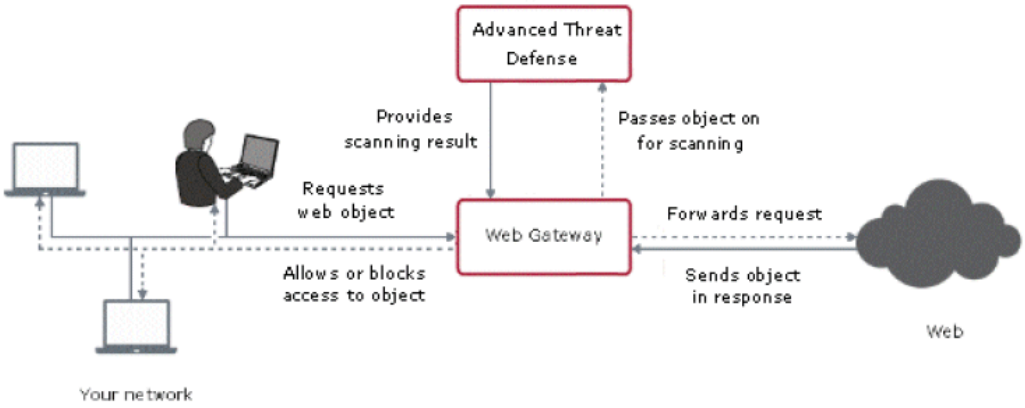


Figure 1-4 Integration with McAfee® Web Gateway

This design ensures that only those files that require an in-depth analysis are sent to McAfee Advanced Threat Defense. This balances your users' experience in terms of download speed and security. For information on how to integrate McAfee Advanced Threat Defense and McAfee® Web Gateway, see the *McAfee® Web Gateway Product Guide,* version 7.4.

- Integration with McAfee® ePolicy Orchestrator (McAfee ePO) — This integration enables McAfee Advanced Threat Defense to retrieve information regarding the target host. Knowing the operating system on the target host, enables it to select a similar virtual environment for dynamic analysis.

How the deployment options address the 4 major aspects of anti-malware process cycle:

- Detection of file download: As soon as a user accesses a file, the inline Network Security Platform Sensor or McAfee® Web Gateway detects this and sends a copy of the file to McAfee Advanced Threat Defense for analysis.
- Analysis of the file for malware: Even before the user fully downloads the file, McAfee Advanced Threat Defense can detect a known malware using sources that are local to it or on the cloud.
- Block future downloads of the same file: Every time McAfee Advanced Threat Defense detects a medium, high, or very high severity malware, it updates its local black list.
- Identify and remediate affected hosts: Integration with Network Security Platform enables you to quarantine the host until it is cleaned up and remediated.

McAfee Advanced Threat Defense advantages

Here are some of the advantages that McAfee Advanced Threat Defense provides:

- It is an on-premises solution that has access to cloud-based GTI. In addition, you can integrate it with other McAfee's security products.
- McAfee Advanced Threat Defense does not sniff or tap into your network traffic. It analyzes the files submitted to it for malware. This means that you can place the McAfee Advanced Threat Defense Appliance anywhere in your network as long as it is reachable to all the integrated McAfee products. It is also possible for one McAfee Advanced Threat Defense Appliance to cater to all such integrated products (assuming the number of files submitted is within the supported level). This design can make it a cost-effective and scalable anti-malware solution.
- McAfee Advanced Threat Defense is not an inline device. It can receive files from IPS Sensors for malware analysis. So, it is possible to deploy McAfee Advanced Threat Defense in such a way that you obtain the advantages of an inline anti-malware solution but without the associated drawbacks.
- Android is currently one of the top targets for malware developers. With this integration, the Android-based handheld devices on your network are also protected. You can dynamically analyze the files downloaded by your Android devices such as smartphones and tablets.
- Files are concurrently analyzed by various engines. So, it is possible for known malware to be blocked in almost real time.
- When McAfee Advanced Threat Defense dynamically analyzes a file, it selects the analyzer virtual machine that uses the same operating system and other applications as that of the target host. This is achieved through its integration with McAfee ePO or through passive device profiling feature of Network Security Platform. This enables you to identify the exact impact on a targeted host, so that you can take the required remedial measures. This also means that McAfee Advanced Threat Defense executes the file only the required virtual machine, reserving its resources for other files.
- Consider a host downloaded a zero-day malware, but a Sensor that detected this file downloaded submitted it to McAfee Advanced Threat Defense. After a dynamic analysis, McAfee Advanced Threat Defense determines the file to be malicious. Based on how you have configured the Advanced Malware policy, it is possible for the Manager to add this malware to the blacklist of all the Sensors in your organization's network. This file also might be on the blacklist of McAfee Advanced Threat Defense. Thus, the chances of the same file re-entering your network is reduced.
- Even the first time when a zero-day malware is downloaded, you can contain it by quarantining the affected hosts until they are cleaned and remediated.

2 Setting up the McAfee Advanced Threat Defense Appliance

Review this chapter for information regarding the McAfee Advanced Threat Defense Appliance and how to set it up.

Contents

- *About McAfee Advanced Threat Defense Appliance*
- *Functions of a McAfee Advanced Threat Defense Appliance*
- *Before you install the McAfee Advanced Threat Defense Appliance*
- *Hardware specifications and environmental requests*
- *Setting up McAfee Advanced Threat Defense*

About McAfee Advanced Threat Defense Appliance

Depending on the model, the McAfee Advanced Threat Defense Appliance is a 1-U or 2-U rack dense chassis with Intel® Xeon® E5-2600 product family processor. The McAfee Advanced Threat Defense Appliance runs on a pre-installed, hardened Linux kernel 3.6.0 and comes preloaded with the McAfee Advanced Threat Defense software.

The McAfee Advanced Threat Defense Appliance is available in the following models:

- ATD-3000: This standard model is a 1U chassis.
- ATD-6000: This high-end model is a 2U chassis.

Functions of a McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliances are purpose-built, scalable, and flexible high-performance servers designed to analyze suspicious files for malware.

The following are the primary functions of the McAfee Advanced Threat Defense Appliance:

- Host the McAfee Advanced Threat Defense software that analyzes files for malware.
- Host the McAfee Advanced Threat Defense web application.
- Host the virtual machines used for dynamic analysis of suspicious files.

For the performance values related to ATD-3000 and ATD-6000, contact McAfee support.

Before you install the McAfee Advanced Threat Defense Appliance

This section describes the tasks that you must complete before you begin to install a McAfee Advanced Threat Defense.

- Read all the provided documentation before installation.
- Make sure that you have selected a suitable location for installing the McAfee Advanced Threat Defense Appliance.
- Check that you have all the necessary equipment and components outlined in this document.
- Familiarize yourself with the McAfee Advanced Threat Defense Appliance network access card (NIC) ports and connectors as described in this document.
- Make sure you have the following information available when you configure the McAfee Advanced Threat Defense Appliance:
  - IPv4 address that you want to assign to the Appliance.
  - Network mask.
  - Default gateway address.

Warnings and cautions

Read and follow these safety warnings when you install the McAfee Advanced Threat Defense Appliance. Failure to observe these safety warnings could result in serious physical injury.

- McAfee Advanced Threat Defense Appliance power on/off — the push-button on/off power switch on the front panel of the McAfee Advanced Threat Defense Appliance does not turn off the AC power. To remove AC power from the McAfee Advanced Threat Defense Appliance, you must unplug the AC power cord from either the power supply or wall outlet for both the power supplies.
- The power supplies in your system might produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system.
- Hazardous conditions — devices and cables: Hazardous electrical conditions might be present on power, telephone, and communication cables. Turn off the McAfee Advanced Threat Defense Appliance and disconnect telecommunications systems, networks, modems, and both the power cords attached to the McAfee Advanced Threat Defense Appliance before opening it. Otherwise, personal injury or equipment damage can result.
- Avoid injury — lifting the McAfee Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the McAfee Advanced Threat Defense Appliance. Doing so invalidates your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Usage restrictions

The following restrictions apply to the use and operation of McAfee Advanced Threat Defense Appliance:

- You should not remove the outer shell of the McAfee Advanced Threat Defense Appliance. Doing so invalidates your warranty.
- The McAfee Advanced Threat Defense Appliance is not a general purpose server.
- McAfee prohibits the use of McAfee Advanced Threat Defense Appliance for anything other than operating the McAfee Advanced Threat Defense solution.
- McAfee prohibits the modification or installation of any hardware or software on the McAfee Advanced Threat Defense Appliance that is not part of the normal operation of McAfee Advanced Threat Defense.

Unpack the shipment

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts as listed in Check your shipment on page 20.
4. Remove the McAfee Advanced Threat Defense Appliance.
5. Place the McAfee Advanced Threat Defense Appliance as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the McAfee Advanced Threat Defense Appliance box.
9. Remove the slide rail kit.
10. Pull out the packing material surrounding the McAfee Advanced Threat Defense Appliance.
11. Remove the McAfee Advanced Threat Defense Appliance from the anti-static bag.
12. Save the box and packing materials for later use in case you need to move or ship the McAfee Advanced Threat Defense Appliance.

Check your shipment

The following accessories are shipped in the McAfee Advanced Threat Defense Appliance crate:

- McAfee Advanced Threat Defense Appliance
- Accessories itemized on the *Content Sheet*
- Set of tool-less slide rails
- Front bezel with key

McAfee Advanced Threat Defense Appliance front and back panels

Figure 2-1 Front view of ATD-3000 with bezel

Figure 2-2 Side view of ATD-3000 without bezel

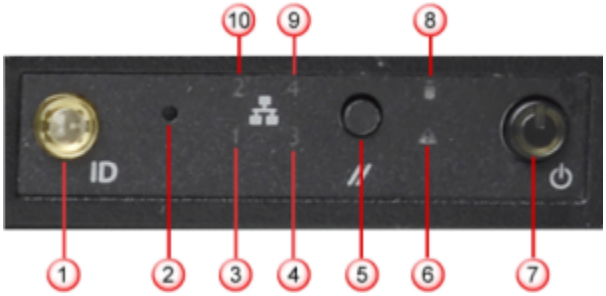


Figure 2-3 ATD-3000 and ATD-6000 front panel

Label	Description
1	System ID button with integrated indicator light
2	NMI button (recessed, tool required for use)
3	NIC 1 activity indicator light
4	• ATD-3000: NIC 3 activity indicator light • ATD-6000: Not used
5	System cold reset button
6	System status indicator light
7	Power button with integrated indicator light
8	Hard drive activity indicator light
9	• ATD-3000: NIC 4 activity indicator light • ATD-6000: Not used
10	NIC 2 activity indicator light

An optional, lockable bezel is included with the McAfee Advanced Threat Defense Appliance, which you can install to cover the front panel.

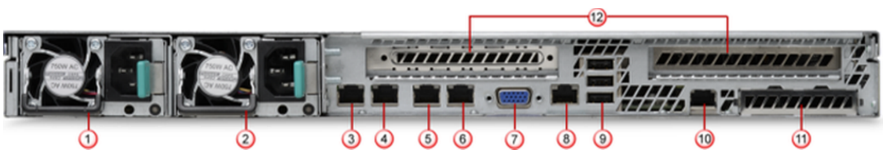


Figure 2-4 ATD-3000 Appliance back panel

Label	Description
1	Power supply module 1
2	Power supply module 2
3	Management port (NIC 1)
4	NIC 2
5	NIC 3
6	NIC 4
7	Video connector
8	RJ45 serial-A port
9	USB ports
10	RMM4 NIC port
11	I/O module ports/connectors (not used)
12	Add-in adapter slots from riser card 1 and riser card 2

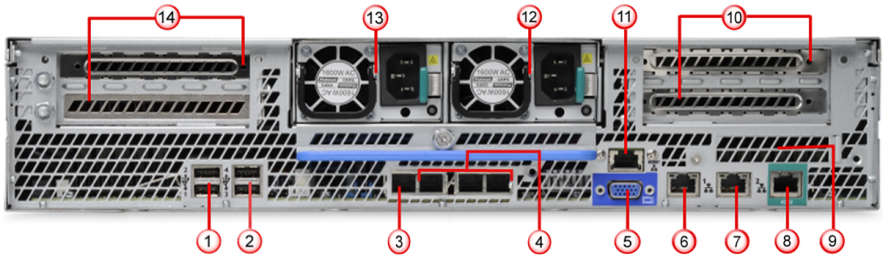


Figure 2-5 ATD-6000 Appliance back panel

Label	Description
1	USB ports
2	USB ports
3	Management port
4	Additional I/O module ports/connectors
5	Video connector
6	NIC 1
7	NIC 2
8	RJ45 serial-A port
9	I/O module ports/connectors (not used)
10	Add-in adapter slots from riser card
11	RMM4 NIC port
12	Power supply module 2
13	Power supply module 1
14	Add-in adapter slots from riser card

Hardware specifications and environmental requests

Specifics	ATD-3000	ATD-6000
Dimensions	• 734.66 L x 438 W x 43.2 H in millimeters • 29 L x 17.25 W x 1.70 H in inches	• 712 L x 438 W x 87.3 H in millimeters • 28 L x 17.24 W x 3.43 H in inches
Form Factor	1U rack mountable; fits 19-inch rack	2U rack mountable; fits 19-inch rack
Weight	15 Kg (33 lbs)	22.7 Kg (50 lbs.)
Storage	• Disk space HDD: 2 x 4TB • SSD: 2 x 400 GB	• Disk space HDD: 4 x 4TB • SSD: 2 x 800 GB
Maximum Power Consumption	2x 750W	2x 1600W
Redundant Power Supply	AC redundant, hot swappable	AC redundant, hot swappable
AC voltage	100 - 240 V at 50 - 60 Hz. 5.8 Amps	100 - 240 V. 50 - 60 Hz. 8.5 Amps
Operating Temperature	+10°C to +35° C (+50°F to + 95°F) with the maximum rate of change not to exceed 10°C per hour	+10º C to +35º C (+50ºF to +95ºF) with the maximum rate of change not to exceed 10°C per hour
Non-operating temperature	-40°C to +70°C (-40°F to +158°F)	-40°C to +70°C (-40°F to +158°F)
Relative humidity (non-condensing)	• Operational: 10% to 90% • Non-operational: 90% at 35°C	• Operational: 10% to 90% • Non-operational: 50% to 90% with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C)
Altitude	Support operation up to 3050 meters (10,000 feet)	Support operation up to 3050 meters (10,000 feet)
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)
Acoustic noise	Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees C).	Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees °C).
Shock, operating	Half sine, 2 g peak, 11 milliseconds	Half sine, 2 g peak, 11 milliseconds
Shock, unpackaged	Trapezoidal, 25 g, velocity change 136 inches/second (≧40 lbs to < 80 lbs)	Trapezoidal, 25 g, velocity change is based on packaged weight
Shock, packaged	Non-palletized free fall in height 24 inches (≧40 lbs to < 80 lbs)	• Product Weight: ≥ 40 to < 80 • Non-palletized Free Fall Height = 18 inches • Palletized (single product) Free Fall Height = NA

Specifics	ATD-3000	ATD-6000
Vibration	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random Packaged: 5 Hz to 500 Hz, 1.09 g RMS random
ESD	+/-12 KV except I/O port +/- 8 KV per Intel® Environmental test specification	Air Discharged: 12.0 kV Contact Discharge: 8.0 kV
System cooling requirement in BTU/Hr	• 460 Watt Max – 1570 BTU/hour • 750 Watt Max – 2560 BTU/hour	• 460 Watt Max – 1570 BTU/hour • 750 Watt Max – 2560 BTU/hour

Port numbers

Table 2-1 Port numbers

Client	Server	Default port	Configurable	Description
Any (desktop)	McAfee Advanced Threat Defense	TCP 443 (HTTPS)	No	Access McAfee Advanced Threat Defense web application
Any (FTP client)	McAfee Advanced Threat Defense	TCP 22 (SFTP)	No	Access the FTP server on McAfee Advanced Threat Defense
Sensor	McAfee Advanced Threat Defense	TCP 8505	No	Communication channel between a Sensor and McAfee Advanced Threat Defense
Manager	McAfee Advanced Threat Defense	TCP (443) (HTTPS)	No	Communication between the Manager and McAfee Advanced Threat Defense through the RESTful APIs.
McAfee Advanced Threat Defense	McAfee ePO	TCP 8443	Yes	Host information queries.
McAfee Advanced Threat Defense	McAfee GTI	TCP (443) (HTTPS)	No	
Any (SSH client)	McAfee Advanced Threat Defense	TCP 2222 (SSH)	No	CLI access

Setting up McAfee Advanced Threat Defense

This chapter describes how to set up the Sensor for you to configure it.

Contents

- *Install or remove rack handles*
- *Install or remove the Appliance from the rack*
- *Turn on the McAfee Advanced Threat Defense Appliance*
- *Handling the front bezel*
- *Connect the network cable*
- *Configure network information for McAfee Advanced Threat Defense Appliance*

Install or remove rack handles

- To install a rack handle, align it with the two holes on the side of the McAfee Advanced Threat Defense Appliance and attach the rack handle to the Appliance with two screws as shown.

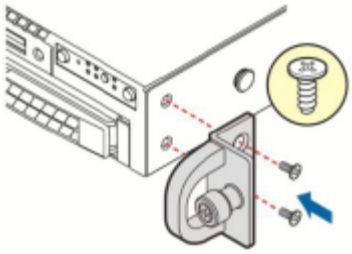


Figure 2-6 Installing the rack handle

- To remove a rack handle, remove the two screws holding the rack handle in place, and remove the rack handle from the server system as shown.

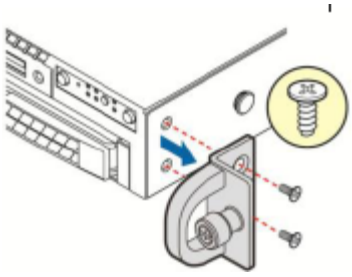


Figure 2-7 Removing the rack handle

Install or remove the Appliance from the rack

Use the rack-mounting kit included with the McAfee Advanced Threat Defense Appliance to install the unit into a four-post 19-inch rack. The kit can be used with most industry-standard rack cabinets. Use the tie wraps to secure the cables from the McAfee Advanced Threat Defense Appliance to the rack.

Task

1 At the front of the rack, position the right or the left mounting rail on the corresponding side so that its mounting bracket aligns with the required rack holes.

Ensure that you follow the safety warnings. When identifying where you want the McAfee Advanced Threat Defense Appliance to go in the rack, remember that you should always load the rack from the bottom up. If you are installing multiple McAfee Advanced Threat Defense Appliances, start with the lowest available position first.

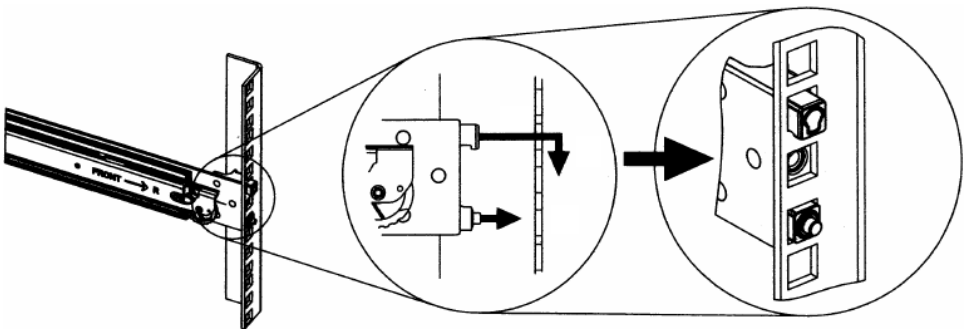


Figure 2-8 Slide rail installation

2 At the back of the rack, pull the back mounting-bracket (extending the mounting rail) so that it aligns with the required rack holes.

Ensure that the mounting rails are at the same level on each side of the rack.

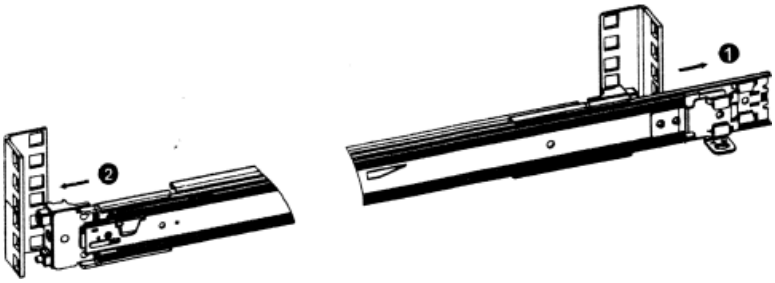


Figure 2-9 Install rail to rack

3 Clip the rail to the rack and secure it.

4 Repeat these steps to secure the second mounting rail to the rack.

5 Slide both the rails to full extent.

Figure 2-10 Full extend slide

6 With help from another person, lift the McAfee Advanced Threat Defense Appliance and install the chassis to the rail simultaneously on both the sides.

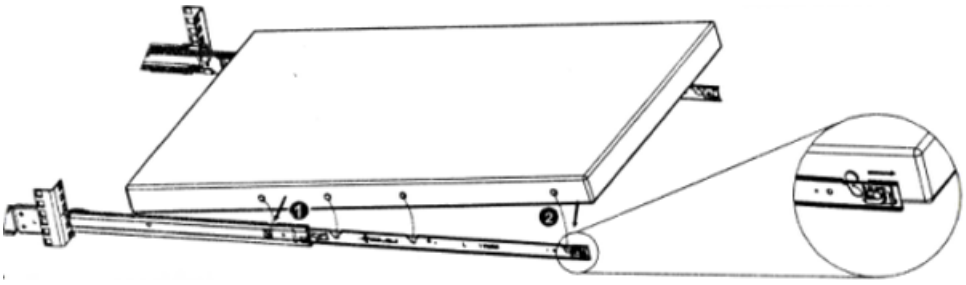


Figure 2-11 Install the Appliance to rail

Drop in the rear spool first, followed by the middle and then front.

Lifting the McAfee Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.

7 Attach the lockable bezel to protect the front panel if required.

8 Lift the release tab and push the Appliance into the rack.

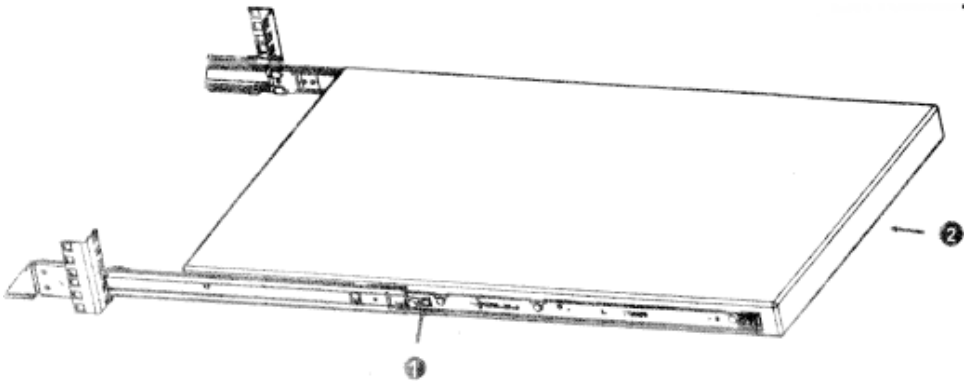


Figure 2-12 Lift release tab and push Appliance into rack

9 To remove the McAfee Advanced Threat Defense Appliance from the rack, lift the release tab next to the front spool on the chassis and lift it out of the rails.

This needs to be done simultaneously on both the sides and requires two people.

Turn on the McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliance has redundant power supplies pre-installed.

The McAfee Advanced Threat Defense Appliance ships with two power cords specific to your country or region.

Task

1 Plug one end of the AC power cord into the first power supply module in the back panel and the other end into an appropriate power source.

2 Plug one end of the AC power cord into the second power supply module in the back panel and the other end into an appropriate power source.

3 Push the power button on the front panel.

The on/off button on the front panel does not turn off the AC power. To remove AC power from the McAfee Advanced Threat Defense Appliance, you must unplug both AC power cords from either the power supply or wall outlet.

Handling the front bezel

You can remove the front bezel if required, and then re-install it. However, before you install the bezel, you must install the rack handles.

Task

1 Follow these steps to remove the front bezel.

   a Unlock the bezel if it is locked.

   b Remove the left end of front bezel from rack handle.

   c Rotate the front bezel anticlockwise to release the latches on the right end from the rack handle.

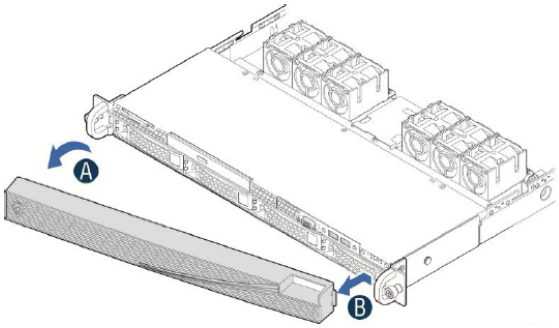


Figure 2-13 Removing front bezel

2 Follow these steps to install the front bezel.

   a Lock the right end of the front bezel to the rack handle

   b Rotate the front bezel clockwise until the left end clicks into place

   c Lock the bezel if needed.

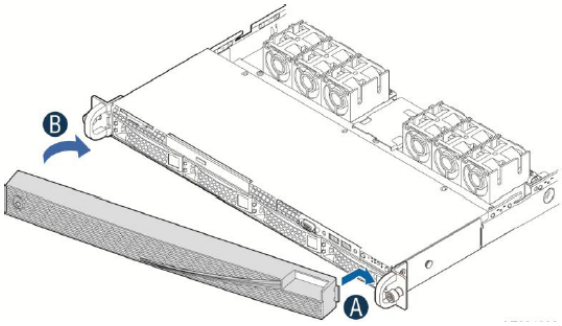


Figure 2-14 Installing front bezel

Connect the network cable

Task

1 Plug a Category 5e or 6 Ethernet cable in the management port, which is located in the back panel.

2 Plug the other end of the cable into the corresponding network device.

Configure network information for McAfee Advanced Threat Defense Appliance

After you complete the initial installation and configuration, you can manage the McAfee Advanced Threat Defense Appliance from a remote computer or terminal server. To do so, you must configure the McAfee Advanced Threat Defense Appliance with the required network information.

Task

1 Plug a console cable (RJ45 to DB9 serial) to the console port (RJ45 serial-A port) at the back panel of the McAfee Advanced Threat Defense Appliance.

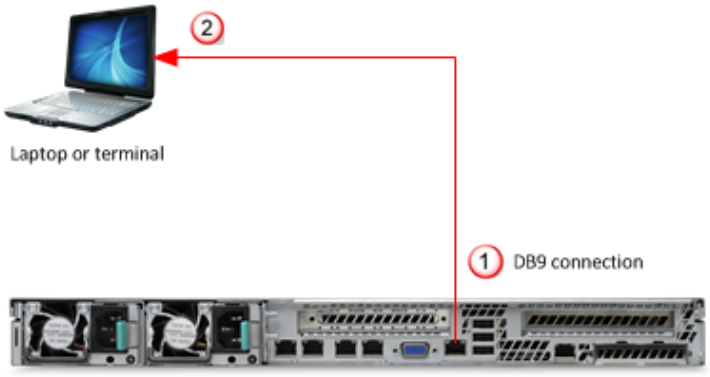


Figure 2-15 Connect the console port

2 Connect the other end of the cable directly to the COM port of the computer or port of the terminal server you are using to configure the McAfee Advanced Threat Defense Appliance.

3 Run the HyperTerminal from a Microsoft Windows-based computer with the following settings.

Name	Setting
Baud rate	115200
Number of Bits	8
Parity	None
Stop Bits	1
Control Flow	None

4 At the logon prompt, log on to the McAfee Advanced Threat Defense Appliance using the default user name atdadmin and password atdadmin.

You can type help or ? to access instructions on using the built-in command syntax help. For a list of all commands, type list.

5 At the command prompt, type set appliance name <Name> to set the name of the McAfee Advanced Threat Defense Appliance.

You need to type the values between <> characters, excluding the <> characters.

Example: set appliance name matd_appliance_1

The McAfee Advanced Threat Defense Appliance name can be an alphanumeric character string up to 25 characters. The string must begin with a letter and can include hyphens, underscores, and periods, but not spaces.

6 To set the management port IP address and subnet mask of the McAfee Advanced Threat Defense Appliance, type set appliance ip <A.B.C.D> <E.F.G.H>

Specify a 32-bit address written as four eight-bit numbers separated by periods as in <A.B.C.D>, where A, B, C, or D is an eight-bit number between 0-255. <E.F.G.H> represents the subnet mask.

Example: set appliance ip 192.34.2.8 255.255.255.0

Setting the IP address for the first time during the initial configuration of the McAfee Advanced Threat Defense Appliance does not require you to restart the McAfee Advanced Threat Defense Appliance. Subsequent changes to the IP address, however, require you to restart the McAfee Advanced Threat Defense Appliance for the changes to take effect.

7 Set the address of the default gateway.

set appliance gateway <A.B.C.D>

Use the same convention as for the set appliance ip command.

Example: set appliance gateway 192.34.2.1

8 Set the port speed and duplex settings for the management port using one of the following commands:

- set mgmtport auto — Sets the management port in auto mode for speed and duplex.
- set mgmtport speed (10|100) duplex (full|half) — Sets the speed to 10 or 100 Mbps at full or half duplex.

9 To verify the configuration, type show.

This displays the current configuration details.

10 To check the network connectivity, ping other network hosts. At the prompt, type ping <IP address>

The success message host <ip address> is alive appears. If the host is not reachable, failed to talk to <ip address> appears.

11 Change the McAfee Advanced Threat Defense Appliance password by using the passwd command.

A password must be between 8 and 25 characters, is case sensitive, and can consist of any alphanumeric character or symbol.

McAfee strongly recommends that you choose a password with a combination of characters that is easy for you to remember but difficult for someone else to guess.

3 Accessing McAfee Advanced Threat Defense web application

The McAfee Advanced Threat Defense web application is hosted on the McAfee Advanced Threat Defense Appliance. If you are a McAfee Advanced Threat Defense user with web access, you can access the McAfee Advanced Threat Defense web application from a remote machine using a supported browser.

Using the McAfee Advanced Threat Defense web application, you can:

- Monitor the state and performance of the McAfee Advanced Threat Defense Appliance.
- Manage McAfee Advanced Threat Defense users and their permissions.
- Configure McAfee Advanced Threat Defense for malware analysis.
- Manually upload files to be analyzed.
- Monitor the progress of the analysis and subsequently view the results.

Contents

- *McAfee Advanced Threat Defense client requirements*
- *Access the McAfee Advanced Threat Defense web application*

McAfee Advanced Threat Defense client requirements

The following are the system requirements for client systems connecting to the McAfee Advanced Threat Defense web application.

- Client operating system —
- Browsers — Internet Explorer 9 and later, Firefox, and Chrome.

Access the McAfee Advanced Threat Defense web application

Task

1 From a client computer, open a session using one of the supported browsers.

2 Use the following to access the McAfee Advanced Threat Defense web application:

- URL — https://<McAfee Advanced Threat Defense appliance host name or IP address>
- Default user name — admin
- Password — admin

3 Click **Log In**.

4 Managing users and performance

You use the McAfee Advanced Threat Defense web application to manage user accounts and monitor the McAfee Advanced Threat Defense Appliance's system health and information.

Contents

- *Managing McAfee Advanced Threat Defense users*
- *Monitoring the McAfee Advanced Threat Defense performance*
- *Import McAfee Advanced Threat Defense software*
- *Troubleshooting*

Managing McAfee Advanced Threat Defense users

You can create user accounts for McAfee Advanced Threat Defense with different permissions and configuration settings. These permissions and settings depend on the user's role with respect to malware analysis using McAfee Advanced Threat Defense. Using the McAfee Advanced Threat Defense web application, you can create user accounts for:

- Users who use the McAfee Advanced Threat Defense web application for submitting files for analysis and for viewing the results of the analysis.
- Users who upload the files to the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Users who directly use the RESTful APIs for uploading files. For more information, see the *McAfee Advanced Threat Defense RESTful APIs Reference Guide.*

In the user record, you also specify the default analyzer profile. If you are using the McAfee Advanced Threat Defense web application to upload, you can override this selection when you actually upload a file.

For each user, you can also configure the FTP server details to which you want McAfee Advanced Threat Defense to upload the results of the analysis.

- There are four default user records.
  - Default admin — This is the default super-user account. You can use this account to initially configure the McAfee Advanced Threat Defense web application. The logon name is *admin* and the default password is *admin*.
  - NSP user — The logon name is *nsp* and the default password is *admin*. This is used by Network Security Platform to integrate with McAfee Advanced Threat Defense.

- ATD admin — This is the default user account to access the FTP server on McAfee Advanced Threat Defense. The user name is *atdadmin* and the password is *atdadmin.*
- McAfee Web Gateway user — This is for the integration between McAfee Web Gateway and McAfee Advanced Threat Defense.

As a precaution, make sure you change the default passwords.

- To access the CLI of McAfee Advanced Threat Defense, you must use *atdadmin* as the logon name and *atdadmin* as the password. You cannot access this user record. You cannot create any other user to access the CLI.

You access the CLI through SSH over port 2222. See Log on to the CLI on page 125.

- If you are a not an admin user, you can view your user record and modify it. To modify your role assignments, you must contact the admin user.

Viewing user profiles

If you are a user with admin role, you can view the existing list of McAfee Advanced Threat Defense users. If you do not have admin role, you can view your user record.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed (based on your role).

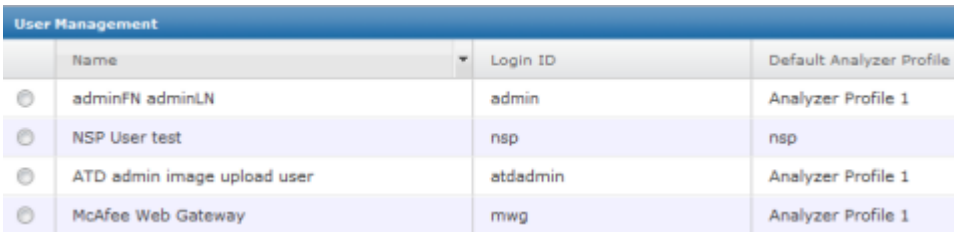


Figure 4-1 View the list of users

Column name	Definition
Select	Select to edit or delete the user record.
Name	Full name of the user as entered in the user details.
Login ID	The user name for accessing McAfee Advanced Threat Defense.
Default Analyzer Profile	The Analyzer Profile that McAfee Advanced Threat Defense uses when the user submits a sample for analysis. However, the user can override this at the time of sample submission.

2 Hide the columns you do not want to see.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

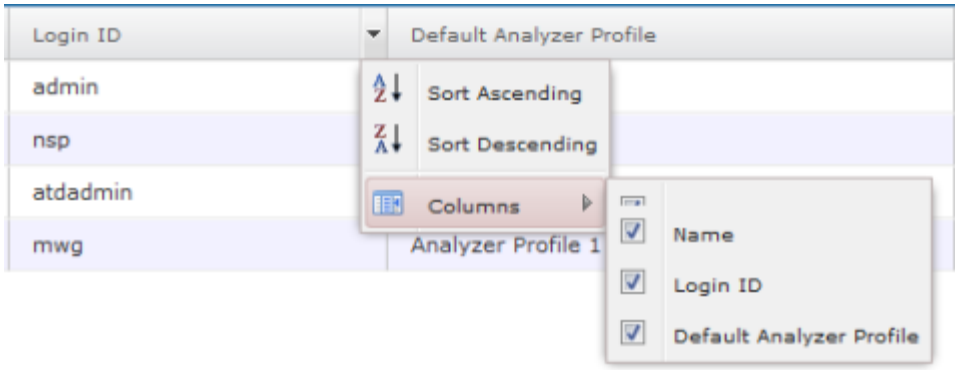


Figure 4-2 Select the required column names

3 To sort the user records list based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific user, select the record and click **Edit**.

Add users

If you have the *admin user* role, you can create the following types of users:

- Users with admin role in the McAfee Advanced Threat Defense web application
- Non-admin users in the McAfee Advanced Threat Defense web application
- Users with access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance
- Access to the RESTful APIs of the McAfee Advanced Threat Defense web application

Task

1 Select **Manage** | **User Management** | **New.**

The **User Management** page is displayed.

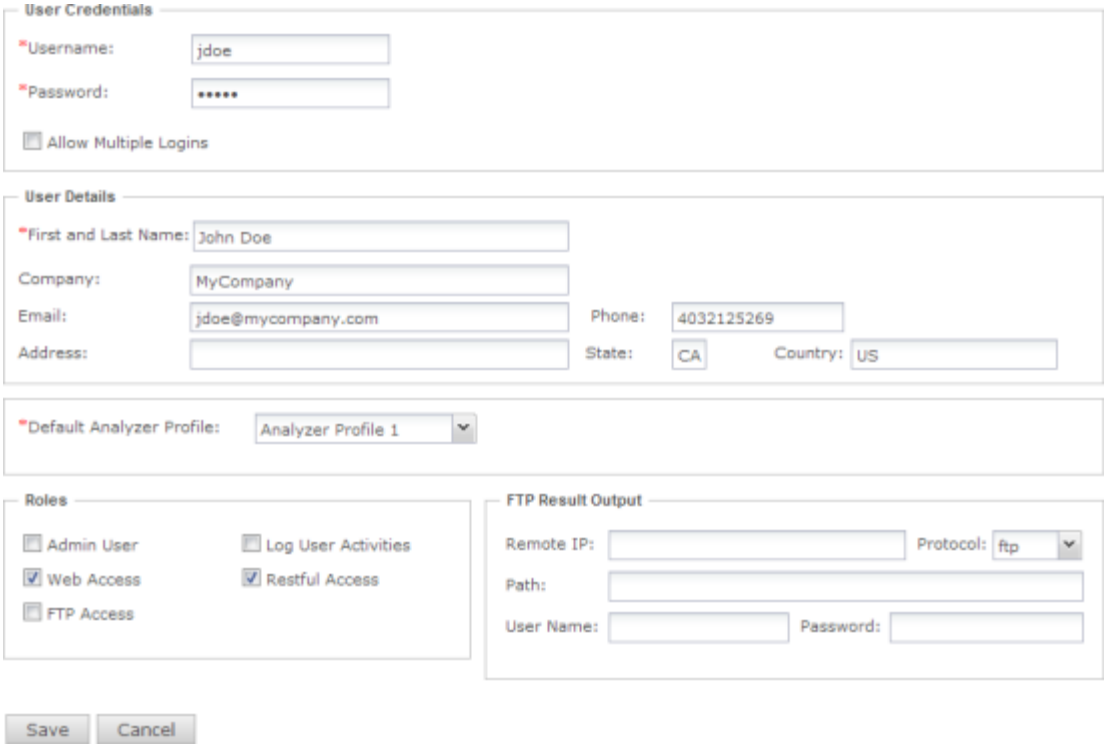


Figure 4-3 Add users

2 Enter the appropriate information in the respective fields.

Option name	Definition
Username	The user name for accessing the McAfee Advanced Threat Defense web application, FTP server, or RESTful APIs.
Password	The default password that you want to provide to the user. It should be of at least 4 characters in length.
Allow Multiple Logins	Deselect it you want to restrict the concurrent logon sessions for this user name to just one. Select if you want to allow multiple concurrent logon sessions for the user name.
First and Last Name	Enter the full name of the user. It should be of at least 2 characters in length.
Email	Optionally, enter the email address of the user.
Company	Optionally, enter the organization to which the user belongs.
Phone	Optionally, enter the user's phone number.
Address	Optionally, enter the user's address for communication.
State	Optionally, enter the corresponding State for the address you entered.
Country	Optionally, enter the corresponding Country for the address you entered.

Option name	Definition
Default Analyzer Profile	Select the analyzer profile that must be used for files submitted by the user. For example, if the file is submitted by a Network Security Platform Sensor, the analyzer profile selected in the *NSP User* record is used. Users, who manually submit files, can override this setting by selecting a different analyzer profile at the time of file submission.
Roles	• **Admin User —** Select to assign super-user rights in the McAfee Advanced Threat Defense web application. Users with this role can access all menus and create other users. • **Web Access —** This role enables a user to submit files using the McAfee Advanced Threat Defense web application and view the results. Users with this role can access all the features but can only view their own user profile. Also, when they manually submit files, they can assign only the analyzer profiles that they created. • **FTP Access —** Select to assign access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance to submit files for analysis and to upload VMDK files. • **Log User Activities —** Select if you want to log the changes made by the user in the McAfee Advanced Threat Defense web application. • **Restful Access —** Select to assign access to the RESTful APIs of the McAfee Advanced Threat Defense web application to submit files for analysis. The **Restful Access** role must be selected for the integrated McAfee products that use RESTful APIs. If you remove this selection, the integration might not work.
FTP Result Output	Specify the details of the FTP server to which McAfee Advanced Threat Defense should provide the results of malware analysis. • **Remote IP —** The IPv4 address of the FTP server. • **Protocol —** Specify whether FTP or SFTP must be used. McAfee recommends using SFTP. • **Path —** The complete path to the folder where the results must be saved. • **User Name —** The user name that McAfee Advanced Threat Defense must use to access the FTP server. • **Password —** The password for accessing the FTP server.
Save	Creates the user record with the information you provided.
Cancel	Closes the **User Management** page without saving the changes.

Edit Users

If you are assigned the admin-user role, you can edit the user profiles. If you intend to modify the mandatory fields, then as a best practice, make sure the corresponding user is not logged on. If you are assigned only the web-access or Restful-access roles, only your user profile is available for editing.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2 Select the required user record and click **Edit**.

The **User Management** page is displayed.

3 Make the changes to the required fields and click **Save**.

For information on the fields, see Add users on page 35.

Delete Users

If you are assigned the admin-user role, you can delete user records. Make sure that the corresponding user is not logged on.

You cannot delete any predefined user records, which are the admin user record, the user record for Network Security Platform, and the user record for McAfee Web Gateway.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2 Select the required user record and click **Delete**.

3 Click **Yes** to confirm deletion.

Monitoring the McAfee Advanced Threat Defense performance

You can use the following options to monitor the performance of McAfee Advanced Threat Defense.

- Use the monitors on the McAfee Advanced Threat Defense dashboard to continuously monitor the performance. See McAfee Advanced Threat Defense performance monitors on page 121.
- Use the status command in the McAfee Advanced Threat Defense Appliance CLI. See CLI commands for McAfee Advanced Threat Defense on page 4.

Import McAfee Advanced Threat Defense software

Before you begin

Make sure that the McAfee Advanced Threat Defense software is extracted and that you can access it from your client computer.

Using the McAfee Advanced Threat Defense web application, you can import the McAfee Advanced Threat Defense software image that you want to upgrade to.

As a precaution, you can use the copyto backup command to copy the software version from the active disk to the backup disk. This enables you to revert to the current software version, if required.

Task

1 Select **Manage** | **Software Management**.

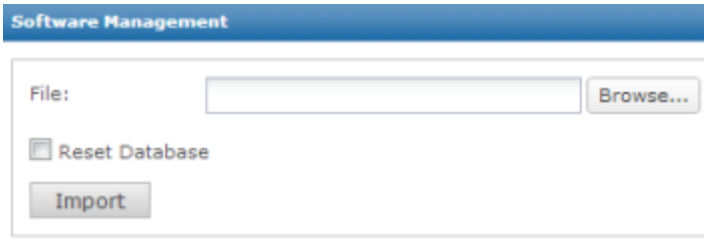


Figure 4-4 McAfee Advanced Threat Defense software upgrade

2 Click **Browse** and select the required McAfee Advanced Threat Defense software.

3 If you want a fresh database to be created as part of the upgrade, select **Reset Database**.

For example, if the database structure is changed in the version that you want to upgrade to, you might need to create a fresh database. If you select this option, a warning message is displayed that all the data from the existing database will be lost. Click **OK** to confirm.

4 Click **Import**.

The McAfee Advanced Threat Defense is upgraded to the selected software. This software is also now stored in the active disk of McAfee Advanced Threat Defense Appliance.

Troubleshooting

The **Troubleshooting** page enables you to complete some tasks related to troubleshooting McAfee Advanced Threat Defense web application. These include exporting logs from McAfee Advanced Threat Defense and clear all the stored analysis results from the McAfee Advanced Threat Defense database.

Task

- To access the **Troubleshooting** page, select **Manage** | **Troubleshooting.**

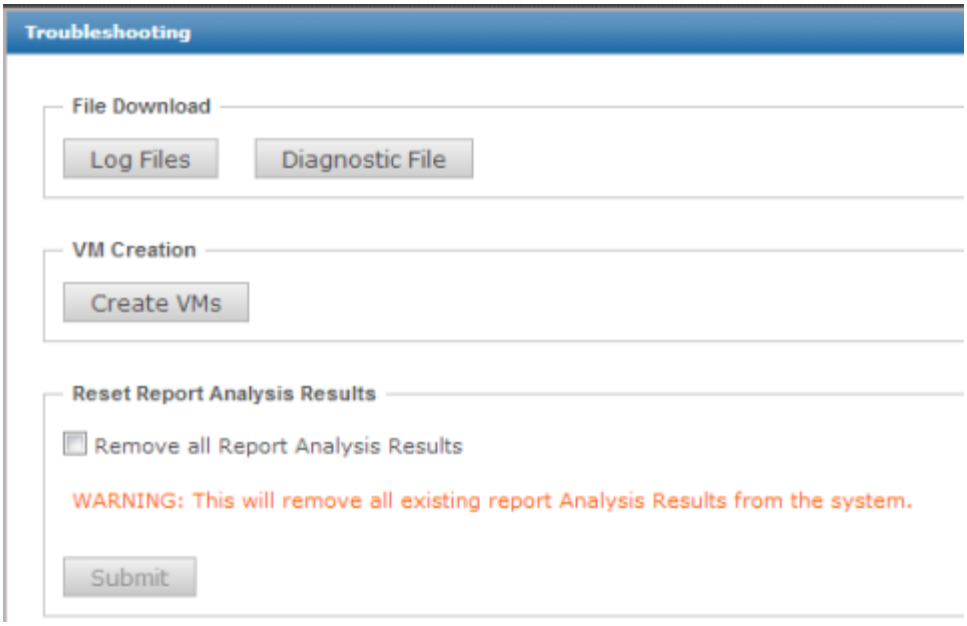


Figure 4-5 Troubleshooting page

Tasks

- *Export McAfee Advanced Threat Defense logs* on page 40
- *Delete the analysis results* on page 40

Export McAfee Advanced Threat Defense logs

If you face issues using McAfee Advanced Threat Defense, you can export the log files and provide them to McAfee support for analysis and troubleshooting. You can export two types of logs — system logs and diagnostic logs. The system logs help to troubleshoot issues related to features, operations, events, and so on. The diagnostic logs are needed to troubleshoot critical issues such as system crashes in McAfee Advanced Threat Defense.

You cannot read the contents of these log files. These are intended for McAfee support.

Task

- In the **Troubleshooting** page, click **Log files** to download the system logs and **Diagnostic File** to download the diagnostic logs.

Delete the analysis results

Task

- In the **Troubleshooting** page, click **Remove all Report Analysis Results** and click **Submit.**

5 Creating analyzer VM

For dynamic analysis, McAfee Advanced Threat Defense executes a suspicious file in a secure virtual machine (VM) and monitors its behavior for malicious activities. This VM is referred to as an analyzer VM. This chapter provides the steps for creating an analyzer VM and the VM profile.

Any security software or low-level utility tool on an analyzer VM, might interfere with the dynamic analysis of the sample file. The sample-file execution might itself be terminated during dynamic analysis. As a result, the reports might not capture the full behavior of the sample file. If you need to find out the complete behavior of a sample file, do not patch the operating system of the analyzer VM or install any security software on it. If you need to find out the effect of the sample file specific to your network, use your Common Operating Environment (COE) image, with the regular security software, to create the analyzer VMs.

The high-level steps for creating an analyzer VM and the VM profile are as follows:

1. Create an ISO image of the corresponding operating system. You must also have the license key for that operating system. For example, to create an Windows 7 analyzer VM, you must have an ISO image of Windows 7 and the license key.
   You can create analyzer VMs running on the following operating systems:
   - Microsoft Windows XP Service Pack 2
   - Microsoft Windows XP Service Pack 3
   - Microsoft Windows Server 2003 Service Pack 1
   - Microsoft Windows Server 2003 Service Pack 2
   - Microsoft Windows Server 2008 64-bit Service Pack 1
   - Microsoft Windows 7 32-bit Service Pack 1
   - Microsoft Windows 7 64-bit Service Pack 1

   The analyzer VM for Android is available by default.
2. Using VMware Workstation 9.0, create a Virtual Machine Disk (VMDK) file of the ISO image. After you create the VM, you can install the required applications such as:
   - Internet Explorer versions 6, 7, 8, 9, and 10.
   - Firefox versions 11, 12, and 13.
   - Microsoft Office versions 2003, 2007, 2010, or 2013.
   - Adobe Reader version 8, 9, or 10.
3. Import the VMDK file into the McAfee Advanced Threat Defense Appliance.
4. Convert the VMDK file into an image (.img) file.
5. Create the VM and the VM profile.

If you already have a VMDK file, it must be a single file that contains all the files required to create the VM.

Contents

- *Create a VMDK file from an ISO image*
- *Import a VMDK file into McAfee Advanced Threat Defense*
- *Convert the VMDK file to an image file*
- *Managing VM profiles*
- *View the VM creation log*

Create a VMDK file from an ISO image

Before you begin

- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of the operating system whose VMDK file you need to create.
- Make sure you have the license key for the operating system.

As an example, this section provides the steps for creating VMDK files from ISO images of Windows XP and Windows 7 using VMware Workstation 9. Creating a Windows 2003 Server VMDK file is similar to Windows XP. Creating a Windows 2008 Server VMDK is similar to Windows 7.

If a particular step is different for Windows 7 and Windows XP, it is mentioned at the start of the step. For common steps, screenshots are provided only for Windows 7.

Task

1. Start the VMware Workstation.
2. In the VMware Workstation page, select **File** | **New Virtual Machine**.

3 In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**

New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
What type of configuration do you want?
Typical (recommended)
Create a Workstation 9.0 virtual machine in a few easy steps.
Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
VMware
Workstation 9
Help
< Back
Next >
Cancel

Figure 5-1 Select the configuration type for the virtual machine

4 In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next.**

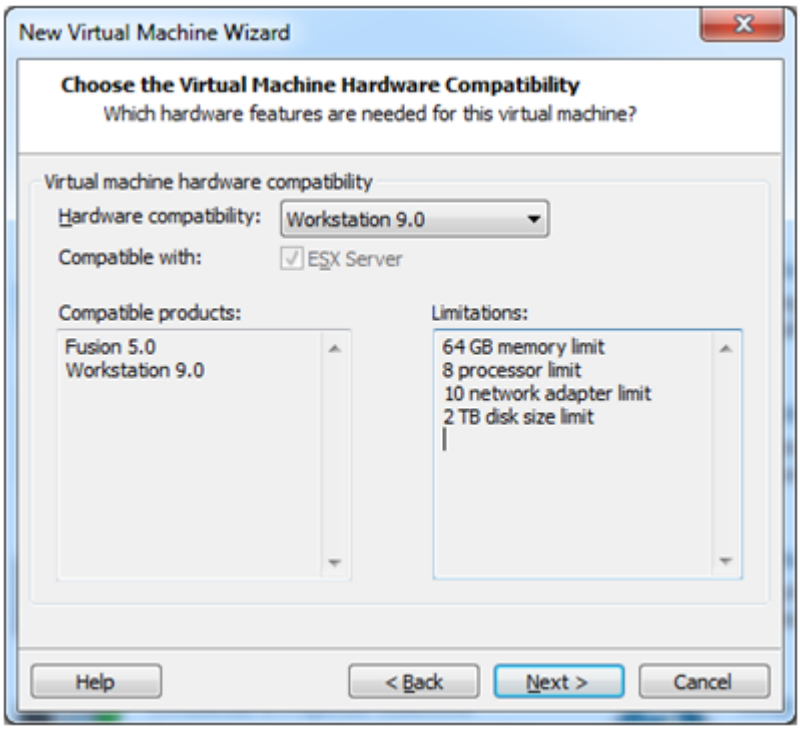


Figure 5-2 Choose the Virtual Machine Hardware Compatibility window

5 In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**.

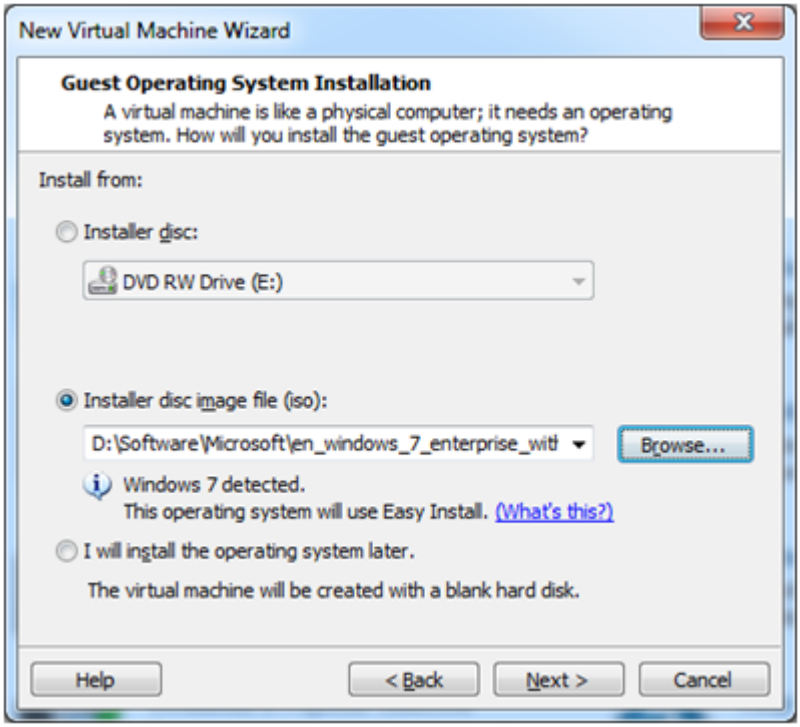

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
DVD RW Drive (E:)
Installer disc image file (iso):
D:\Software\Microsoft\en_windows_7_enterprise_with
Browse...
Windows 7 detected.
This operating system will use Easy Install. (What's this?)
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

Figure 5-3 Guest Operating System Installation window

6 Complete the following in the **Easy Install Information** window and then click **Next**.

- **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file.
- **Version of Windows to install** — Select the corresponding edition of Windows 7 or Windows XP as applicable.
- **Full name** — Enter administrator
- **Password** — Enter cr@cker42

- **Confirm** — Enter cr@cker42
- **Log on automatically (requires a password)** — Deselect this box.

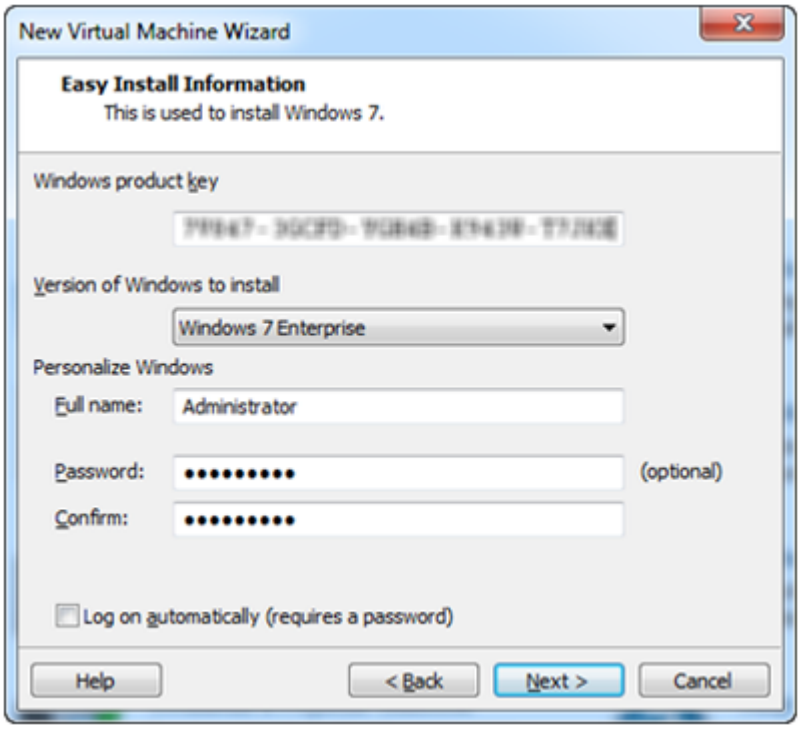


Figure 5-4 Easy Install Information window

7 In the **VMware Workstation** message, click **Yes**.

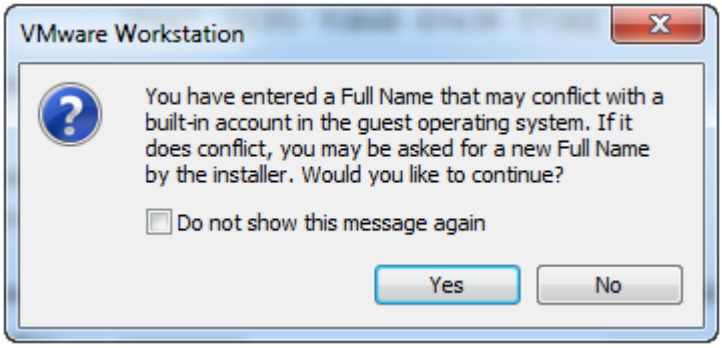

VMware Workstation
You have entered a Full Name that may conflict with a built-in account in the guest operating system. If it does conflict, you may be asked for a new Full Name by the installer. Would you like to continue?
Do not show this message again
Yes
No

Figure 5-5 VMware Workstation message

8 Complete the following in the **Name the Virtual Machine** window and then click **Next**.

- **Virtual Machine name** — Enter virtualMachineImage
- **Location** — Browse and select the folder where you want to create the VMDK file.

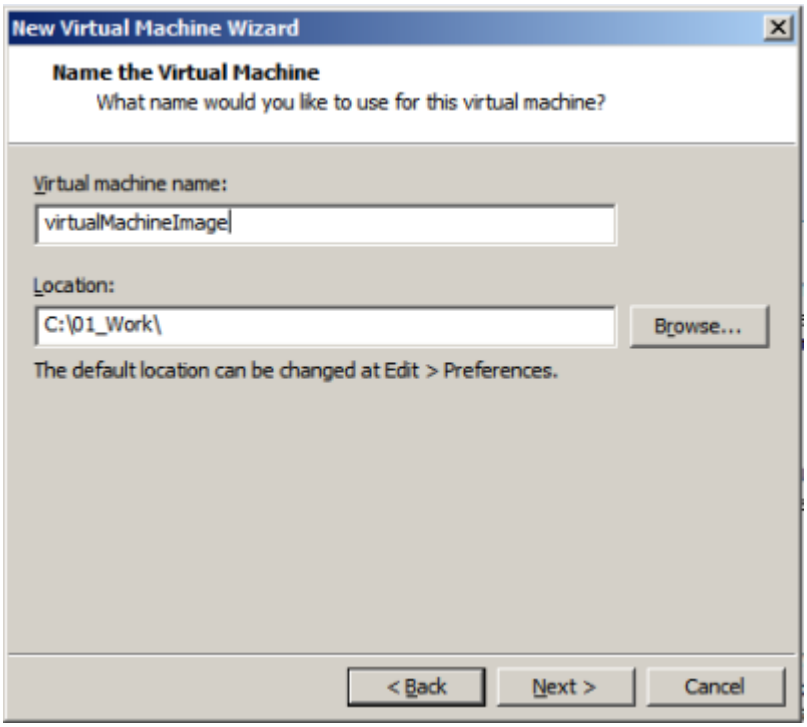


Figure 5-6 Name the Virtual Machine window

9 Leave the default values and click **Next** for the following unless specified otherwise:

- **Processor Configuration**

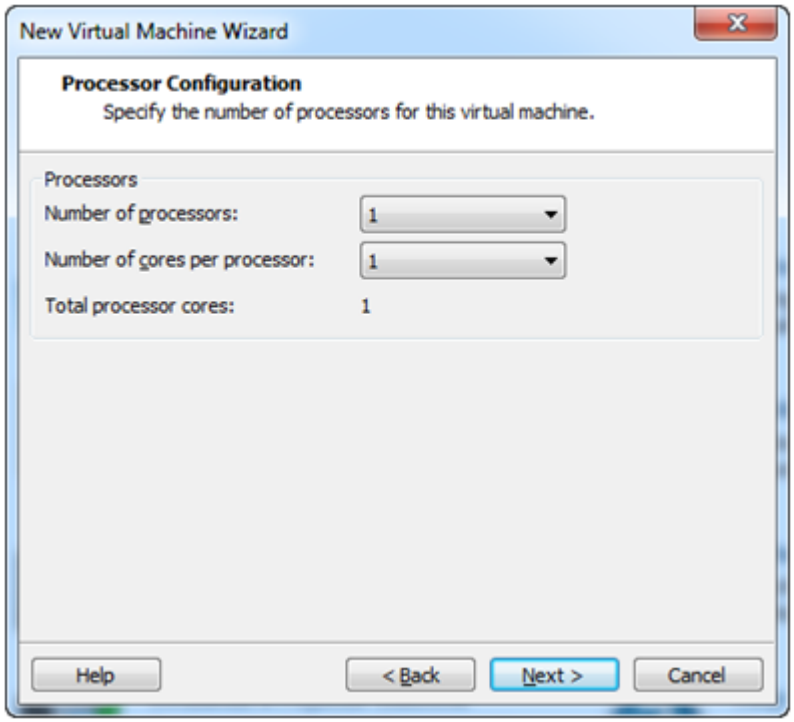


Figure 5-7 Processor configuration for the VM

- **Memory for the Virtual Machine**

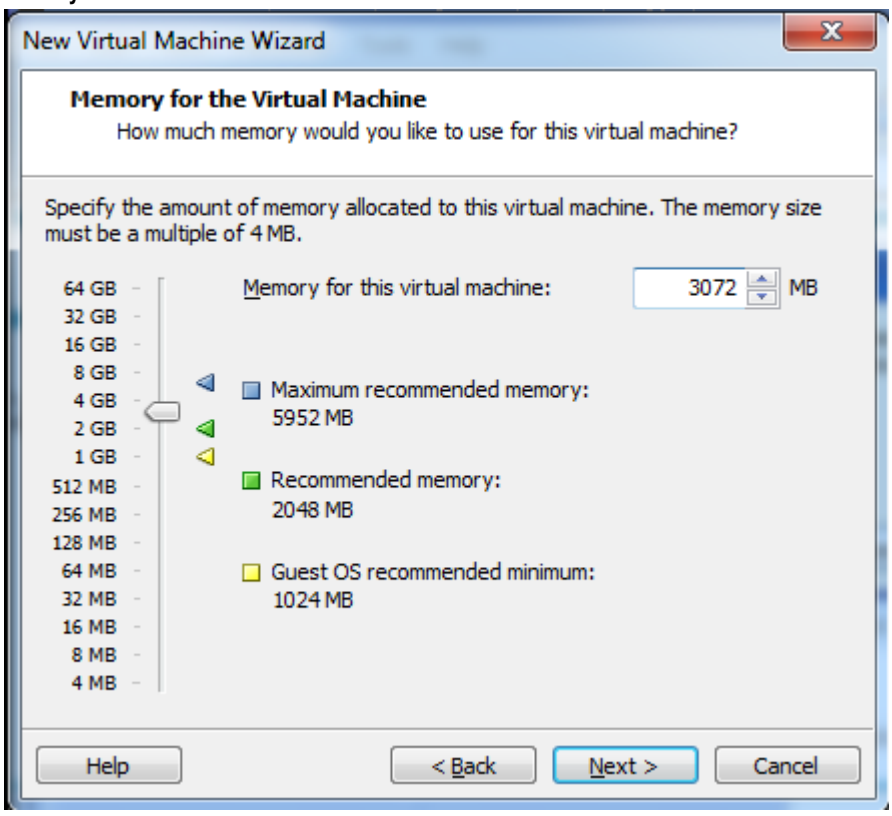


Figure 5-8 Memory configuration for the VM

For Windows XP set 1024 MB as the memory. For Windows 7, set 3072 MB as the memory.

- **Network Type**

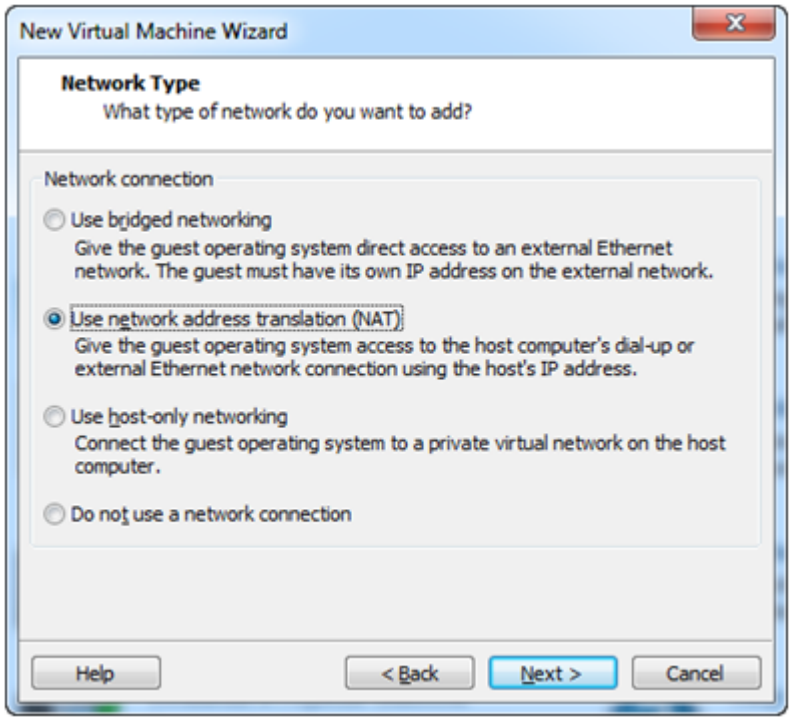

New Virtual Machine Wizard
Network Type
What type of network do you want to add?
Network connection
Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.
Do not use a network connection
Help
< Back
Next >
Cancel

Figure 5-9 Network type configuration for the VM

- **Select I/O Controller Types**

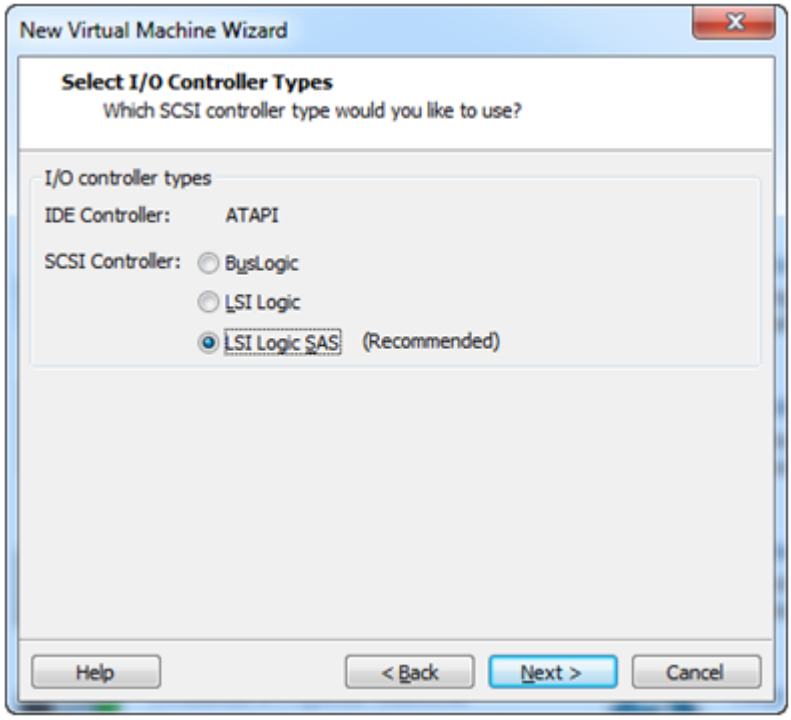


Figure 5-10 Select the I/O controller type

10 In the **Select a Disk Type** page, select **IDE** and click **Next.**

SCSI disks are not compatible with McAfee Advanced Threat Defense.

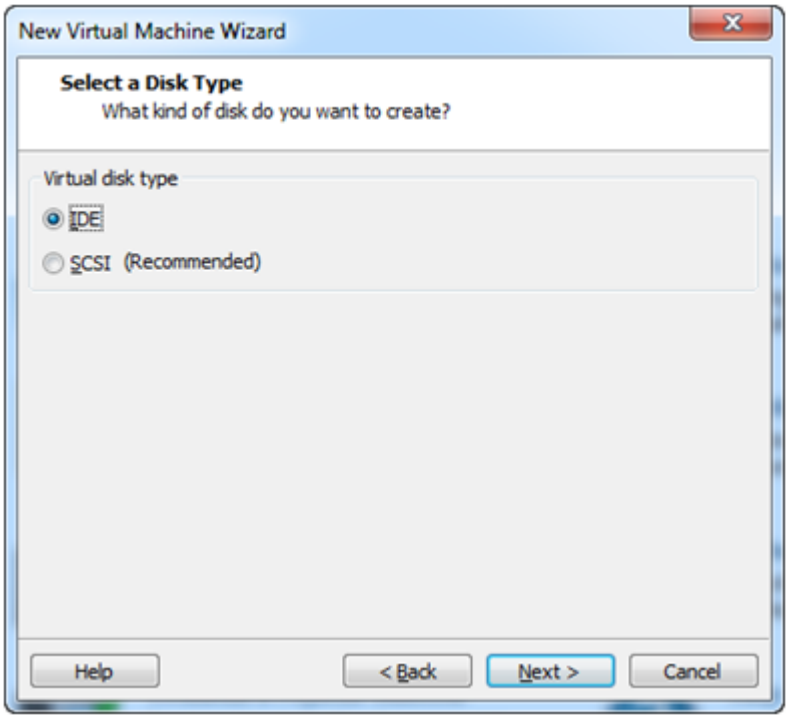


Figure 5-11 Select a disk type

11 In the **Select a Disk** window, select **Create a new virtual disk** and click **Next.**

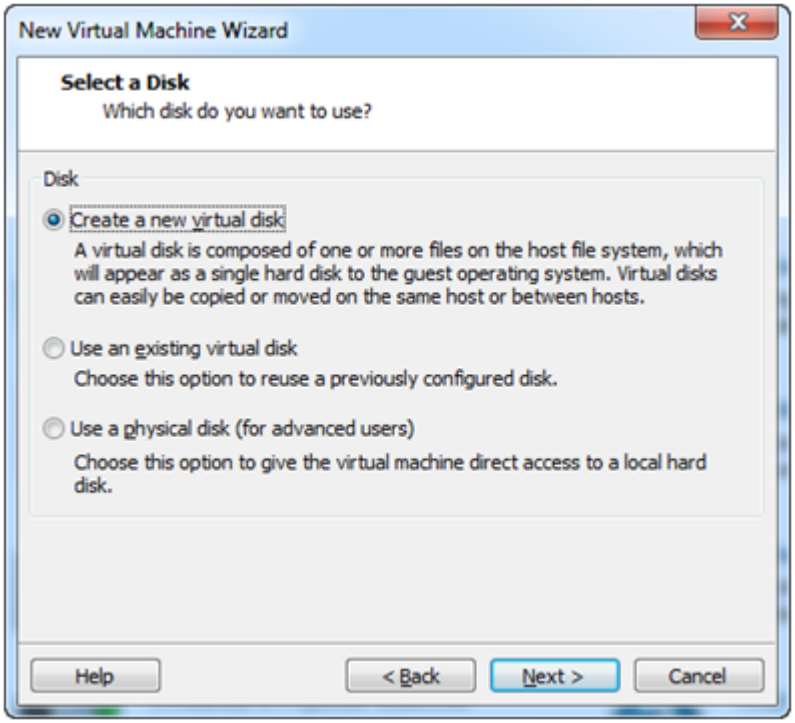

New Virtual Machine Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.
Help
< Back
Next >
Cancel

Figure 5-12 Select a disk

12 Complete the following in the **Specify Disk Capacity** window and then click **Next**.

- **Maximum disk size (GB)** — Enter the exact values mentioned here based on the operating system. For Windows 7 64-bit, you must enter 14 GB. For Windows 7 32-bit, you must enter 12 GB. For Windows XP, you must enter 5 GB.
- Select **Allocate all disk space now**.
- Select **Store virtual disk as a single file**.

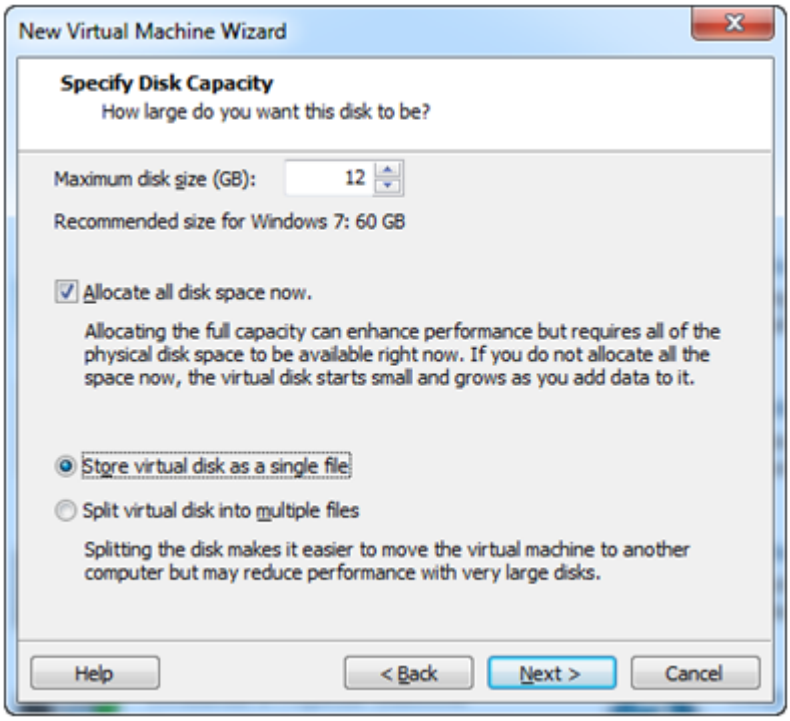

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB):
12
Recommended size for Windows 7: 60 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

Figure 5-13 Specify disk capacity

13 In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**.

If you specified a different name for **Virtual Machine name**, that name is displayed here.

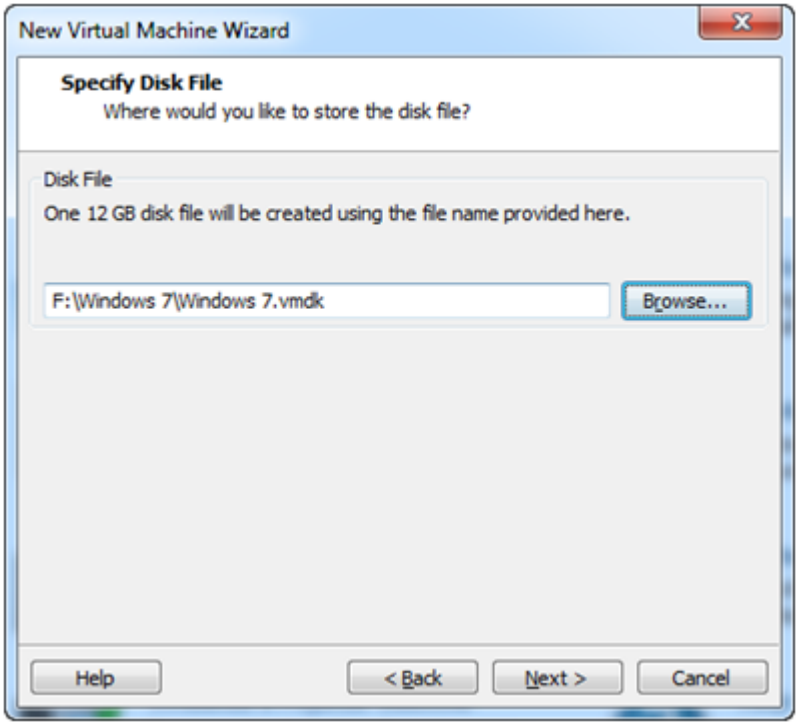

New Virtual Machine Wizard
Specify Disk File
Where would you like to store the disk file?
Disk File
One 12 GB disk file will be created using the file name provided here.
F:\Windows 7\Windows 7.vmdk
Browse...
Help
< Back
Next >
Cancel

Figure 5-14 Specify the path to store the disk file

14 Complete the following in the **Ready to Create Virtual Machine** window.

- **Power on this virtual machine after creation** — Select this option.
- Click **Finish**.

This step might take around 30 minutes to complete.

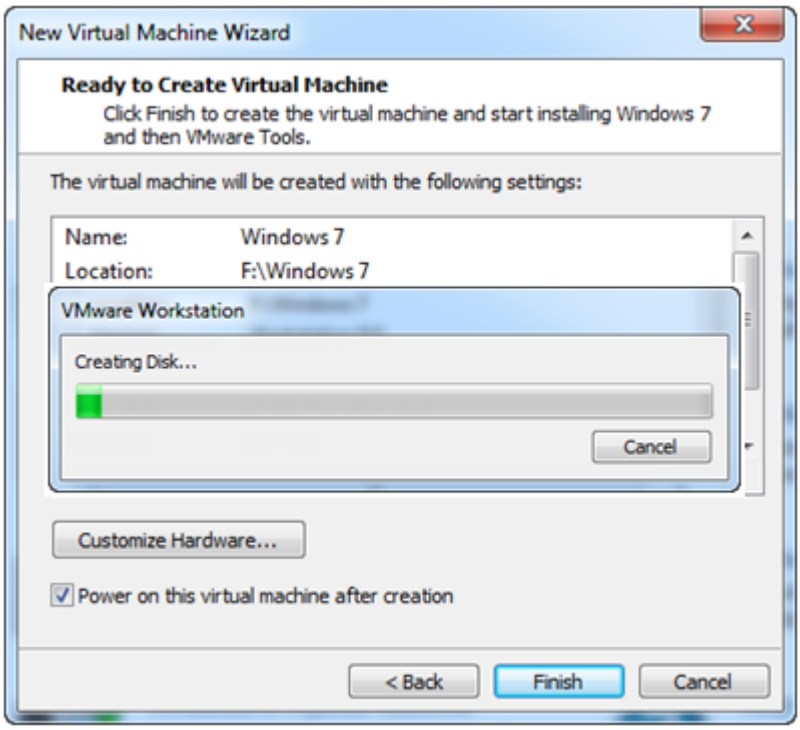

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Windows 7 and then VMware Tools.
The virtual machine will be created with the following settings:
Name: Windows 7
Location: F:\Windows 7
VMware Workstation
Creating Disk...
Cancel
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel

Figure 5-15 VM creation progress

15 If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**.

Windows begins to install, which might take around 15 minutes.

16 Stop the VMware Tools installation.

The VMware Tools are not compatible with McAfee Advanced Threat Defense.

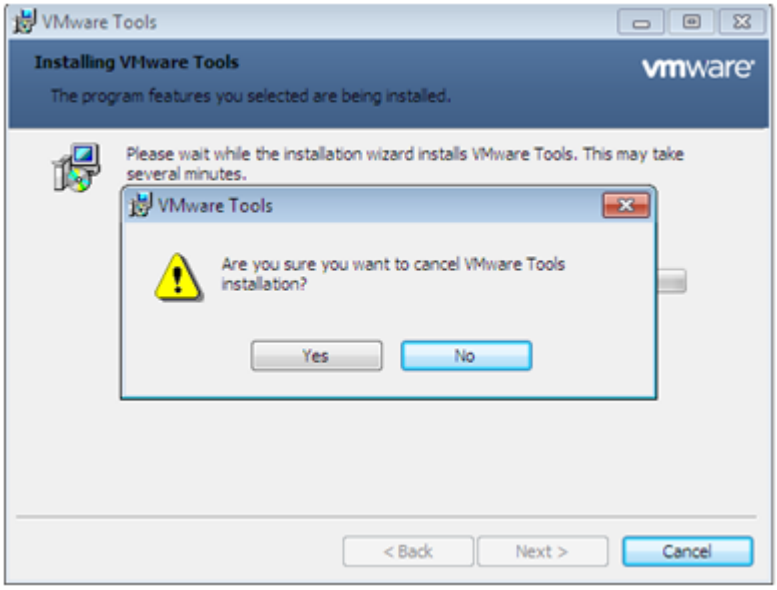

VMware Tools
Installing VMware Tools
The program features you selected are being installed.
vmware
Please wait while the installation wizard installs VMware Tools. This may take several minutes.
VMware Tools
Are you sure you want to cancel VMware Tools installation?
Yes
No
< Back
Next >
Cancel

Figure 5-16 Cancel VMware Tools installation

17 Select **Public network** in the **Set Network Location** window and click **Next**.

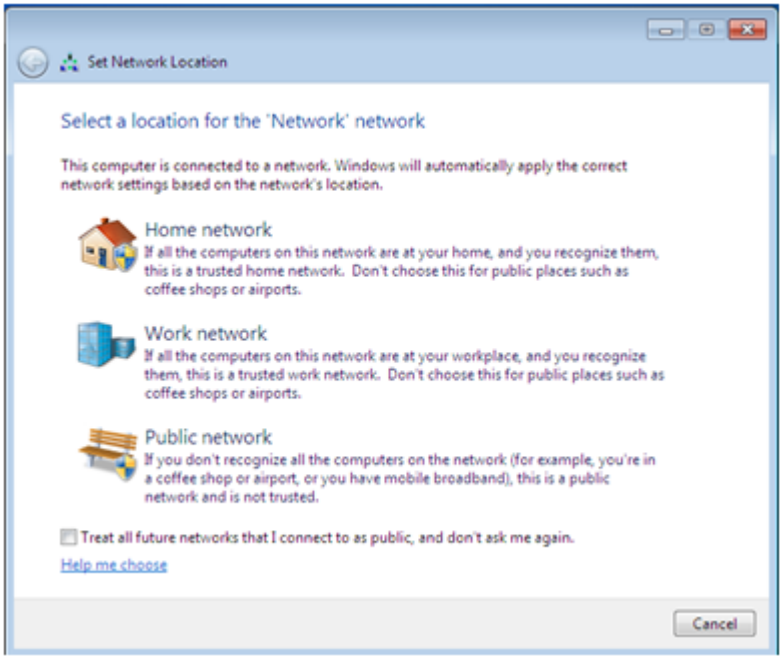

Set Network Location
Select a location for the 'Network' network
This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.
Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.
Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.
Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.
Treat all future networks that I connect to as public, and don't ask me again.
Help me choose
Cancel

Figure 5-17 Select a network location

18 Complete the following only for Windows XP.

a Click **OK** if the following error message is displayed — *Setup cannot continue until you enter your name. Administrator and Guest are not allowable names to use.*

b Enter the following details in the **Windows XP Professional Setup** page.

- **Name:** Enter root
- **Organization:** Leave this blank and click **Next**.

  This operation might take around 15 minutes.

19 Only if prompted, log on to virtualMachineImage with the following credentials.

- **User:** administrator
- **Password:** cr@cker42

20 For Windows XP, in the virtualMachineImage, select **Start** | **Control Panel** | **Security Center** | **Windows Firewall** | **OFF**.

21 For Windows 7, in the virtualMachineImage, complete the following.

a Select **Start** | **Control Panel** | **System and Security** | **Windows Firewall** | **Turn on Windows Firewall On or Off.**

b Select **Turn off Windows Firewall (not recommended)** for both **Home or work(private) network location settings** and **Public network location settings** and then click **OK.**

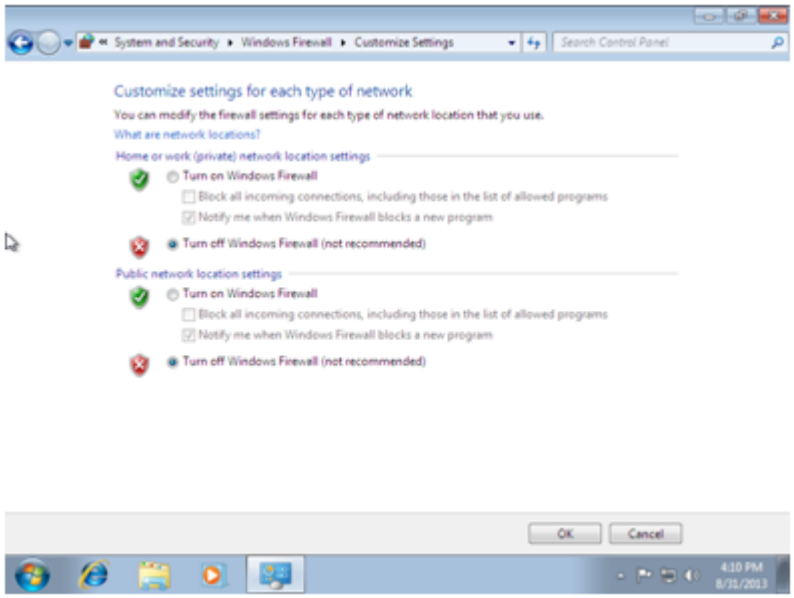

System and Security ▸ Windows Firewall ▸ Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network location that you use.
What are network locations?
Home or work (private) network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
Public network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
OK
Cancel
4:10 PM
8/31/2013

Figure 5-18 Turn off Windows Firewall on the Windows 7 VM

c Select **Start** | **Control Panel** | **Programs** | **Programs and Features** | **Turn Windows feature on or off** and complete the following.

1 Select **Internet Information Services** | **FTP server** and select **FTP Extensibility**.

2 Select **Internet Information Services** | **Web Management Tools** and select **IIS Management Service**.

3 Select **Telnet Server** and press OK.

This operation might take around 5 minutes to complete.

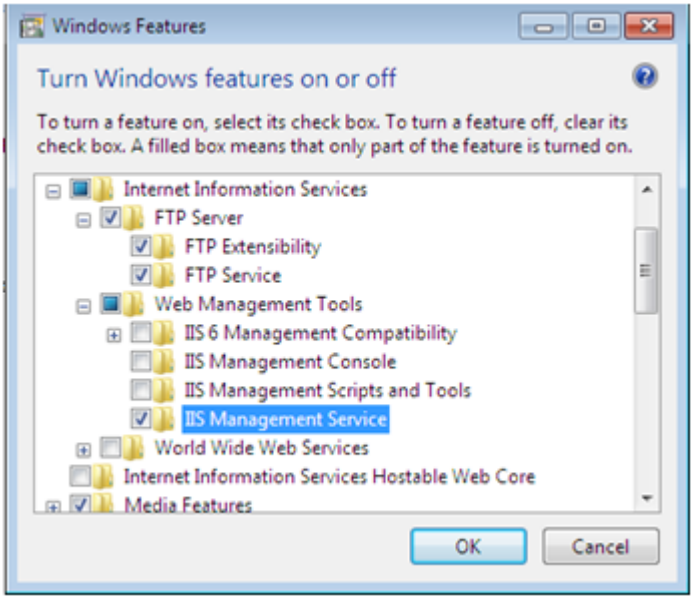

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Internet Information Services
FTP Server
FTP Extensibility
FTP Service
Web Management Tools
IIS 6 Management Compatibility
IIS Management Console
IIS Management Scripts and Tools
IIS Management Service
World Wide Web Services
Internet Information Services Hostable Web Core
Media Features
OK
Cancel

Figure 5-19 Select FTP Server and IIS Management Service options

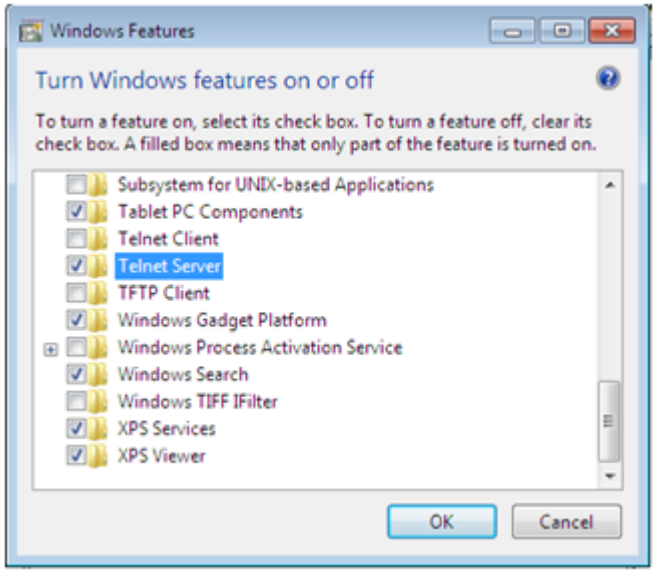

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Subsystem for UNIX-based Applications
Tablet PC Components
Telnet Client
Telnet Server
TFTP Client
Windows Gadget Platform
Windows Process Activation Service
Windows Search
Windows TIFF IFilter
XPS Services
XPS Viewer
OK
Cancel

Figure 5-20 Select Telnet Server option

d Click **Start** and right-click **Computer**. Then select **Manage** | **Services and Applications** | **Services**. Then double-click **Telnet**.

22 For Windows XP, in the virtualMachineImage VM, click **Start** and right-click **My Computer**. Then select **Manage** | **Services and Applications** | **Services**. Then double-click **Telnet**.

23 In the **Telnet Properties(Local Computer)** window, you must select **Automatic** from the **Startup type** drop-down list. Then select **Apply** | **Start** | **OK**.

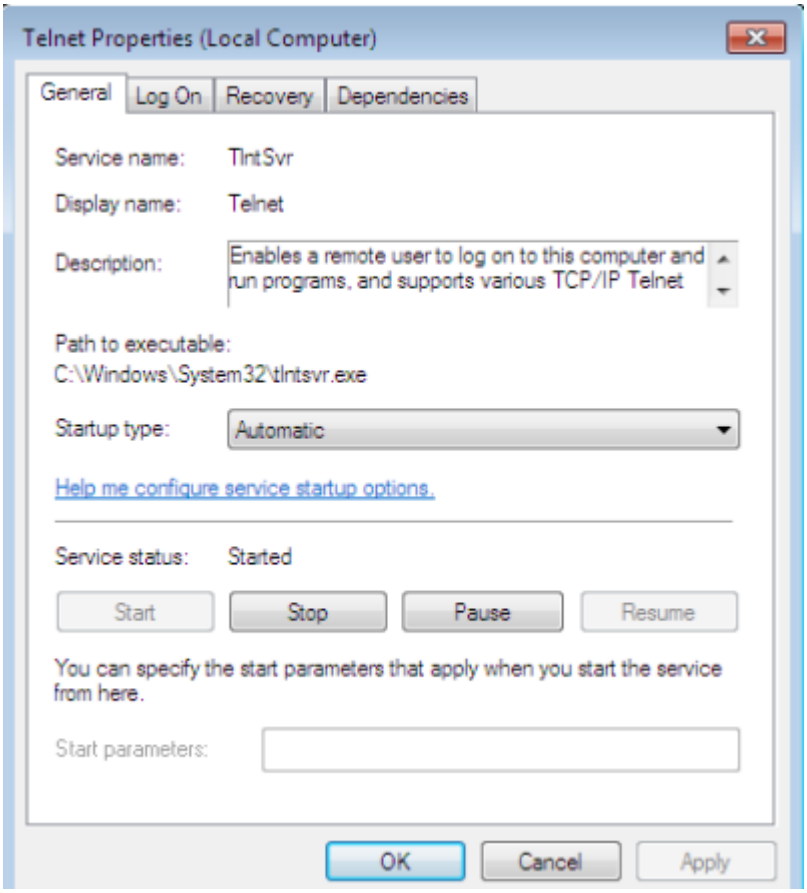


Figure 5-21 Telnet Properties(Local Computer) window

24 To enable FTP on Windows XP, complete the following.

a In the virtualMachineImage, select **Start** | **Control Panel** | **Add or remove Programs** | **Add or remove Windows components**.

b In the **Windows Components** wizard, double-click **Internet Information Services(IIS)**.

c In the **Internet Information Services(IIS)** pop-up window, complete the following.

1 Select **File Transfer Protocol (FTP) Service**.

2 Select **Common Files**.

3 Select **Internet Information Services Snap-In**, click **OK**, and then click **Next**.

d In the **Windows Components** wizard, click **Finish** to finish installing FTP.

e Select **Start** | **Control Panel** | **Administrative Tools** and double-click or expand **Internet Information Services**.

f Expand **FTP Sites**.

g Select **Default FTP Site** | **Properties** | **Home Directory** and complete the following.

1 Browse to C:/

2 Select **Read**.

3 Select **Write**.

4 Select **Log visits** and click **Apply** and then **OK**.

25 To enable FTP on Windows 7, complete the following.

a In the virtualMachineImage, select **Start** | **Control Panel** | **System and Security** | **Administrative Tools**. Double-click **Internet Information Services(IIS)**, expand the tree under **Hostname**, and complete the following:

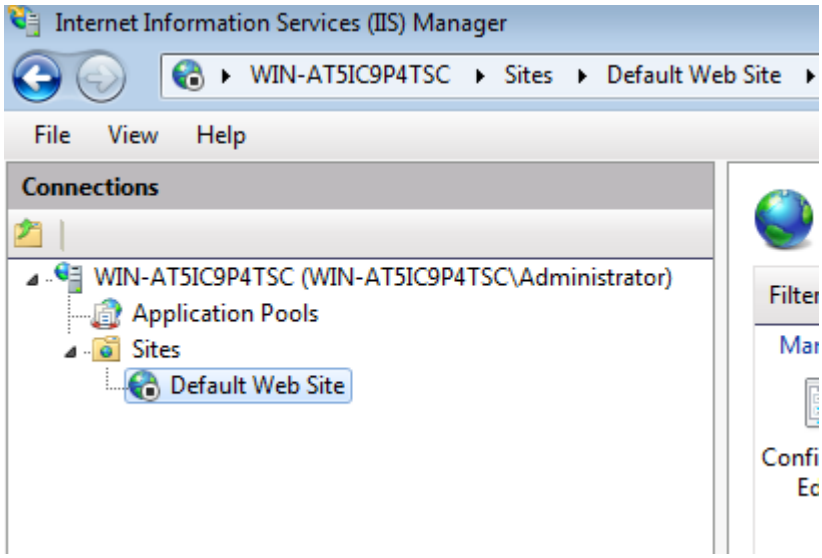


Figure 5-22 Navigate to Default Web Site

1 Select **Sites** and right-click **Default Web Site** and remove. Confirm by clicking **Yes.**

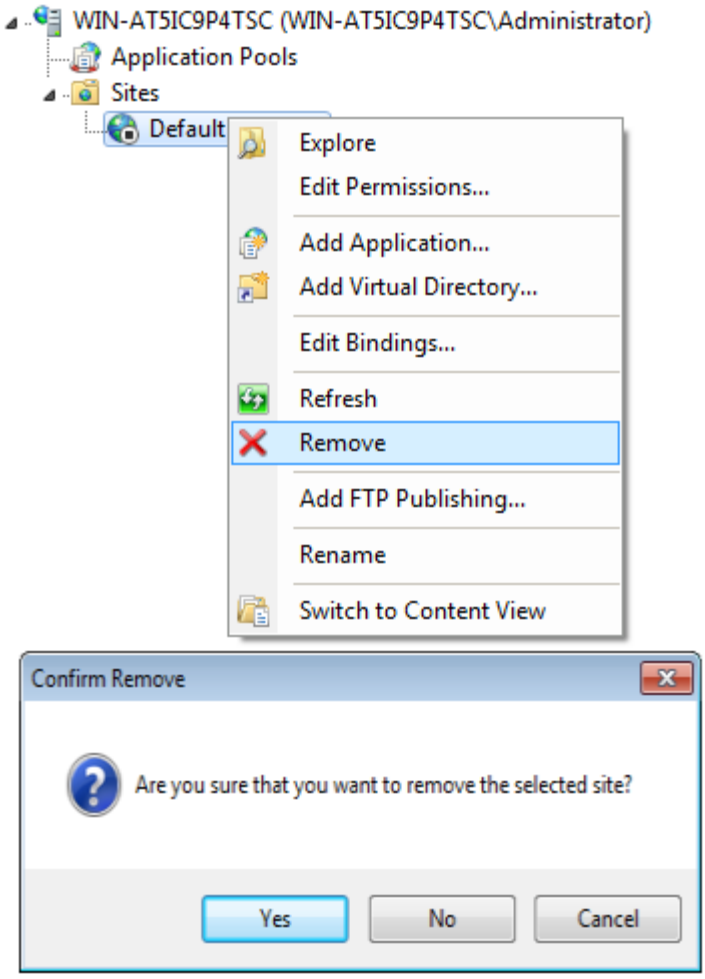


Figure 5-23 Remove Default Web Site

2 Right-click **Sites** and select **Add FTP Site**. Then complete the following.

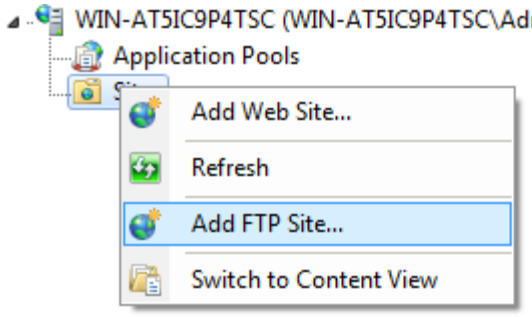


Figure 5-24 Select Add FTP Site

a For **FTP site name**, enter root.

b **Physical Path: C:\.**

c Click **Next**.

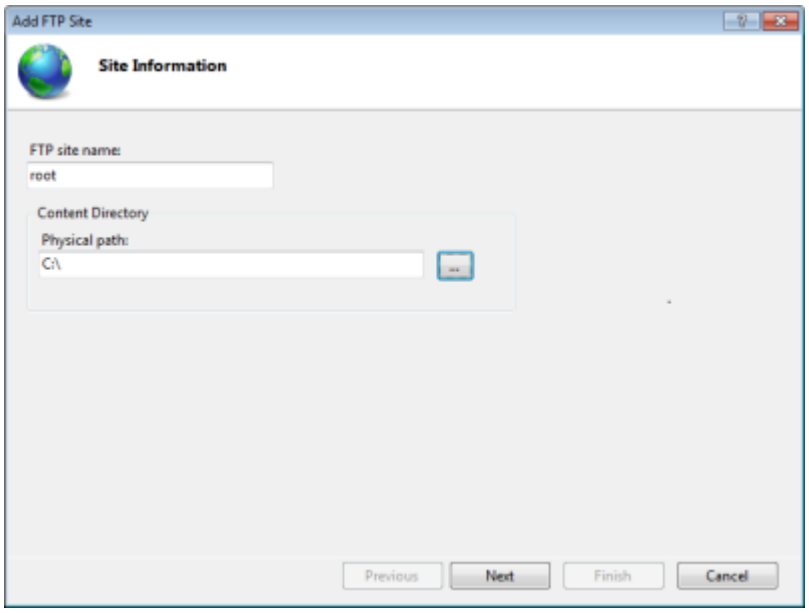


Figure 5-25 Provide the FTP site information

3 For **Bindings and SSL Settings**, select **No SSL**. For all other fields, leave the default values and click **Next**.

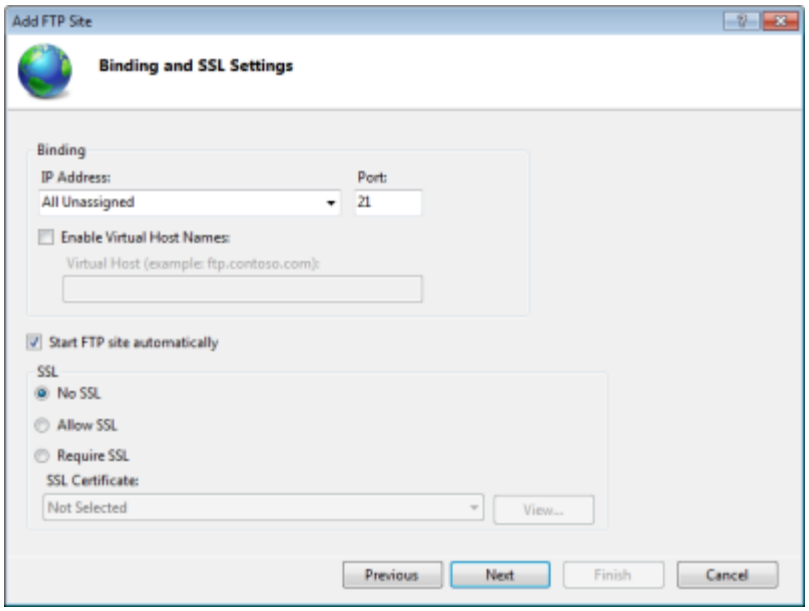


Figure 5-26 Binding and SSL settings

4 For **Authentication and Authorization Information** complete the following.

a Select **Basic**.

b For **Allow access to**, select **All Users**.

c For **Permissions**, select both **Read** and **Write**, and then click **Finish**.

d Close the **Internet Information Services (IIS) Manager**.

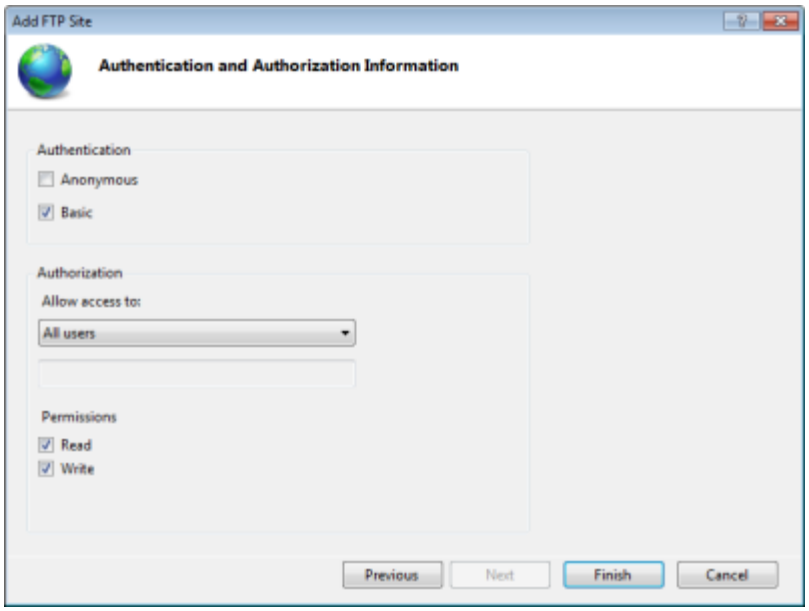


Figure 5-27 Authentication and Authorization Information

26 Set automatic logon.

a For Windows XP, select **Start** | **Run**, enter rundll32 netplwiz.dll,UsersRunDll and press Enter.

b For Windows 7, select **Start** | **Run**, enter netplwiz and press Enter.

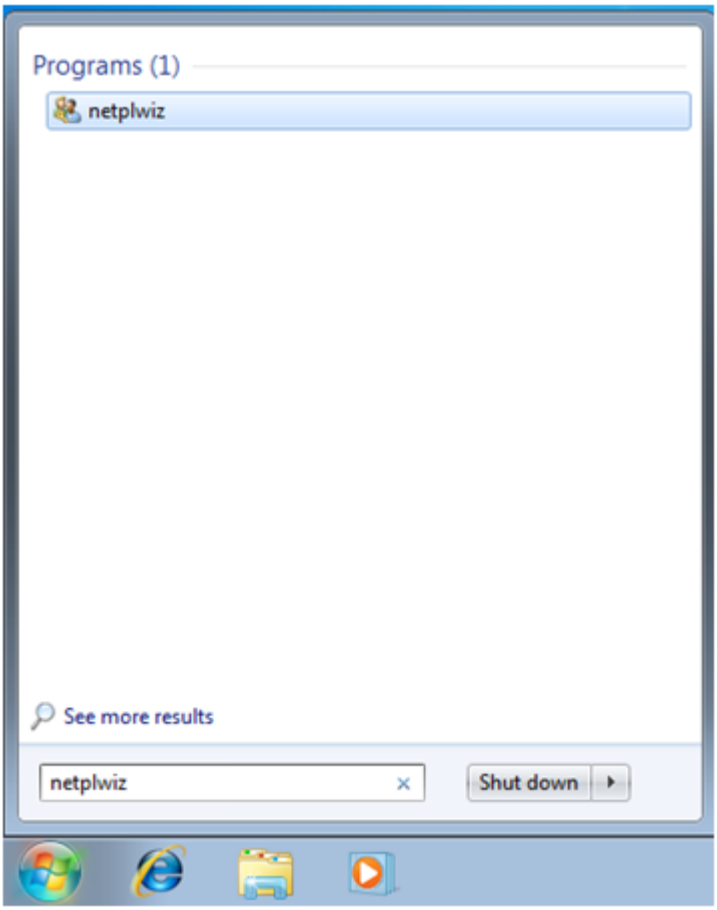


Figure 5-28 Set automatic logon

27 In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**.

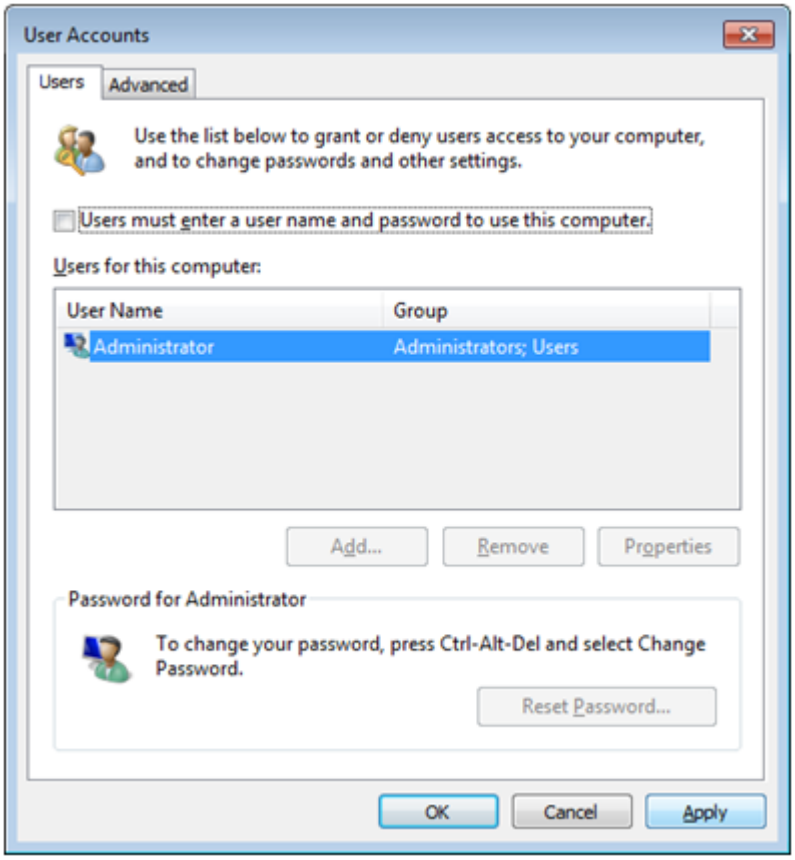


Figure 5-29 User Accounts window

28 In the **Automatically Log On** pop-up window, complete the following.

- **User name** — Enter Administrator
- **Password** — Enter cr@cker42
- **Confirm Password** — Enter cr@cker42

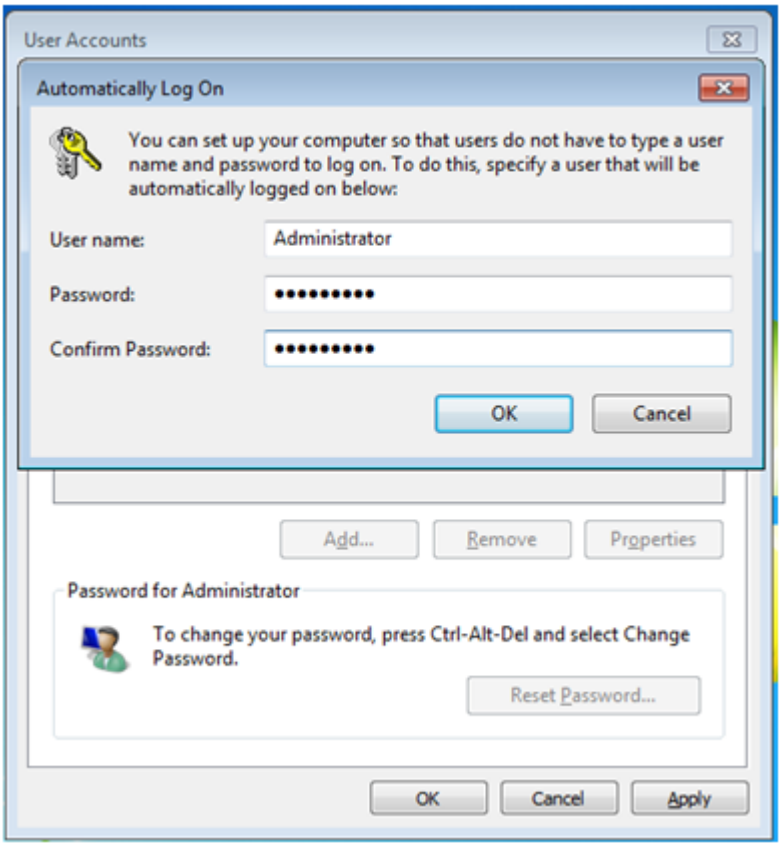


Figure 5-30 Credentials for automatic logon

Press **OK** in the message boxes.

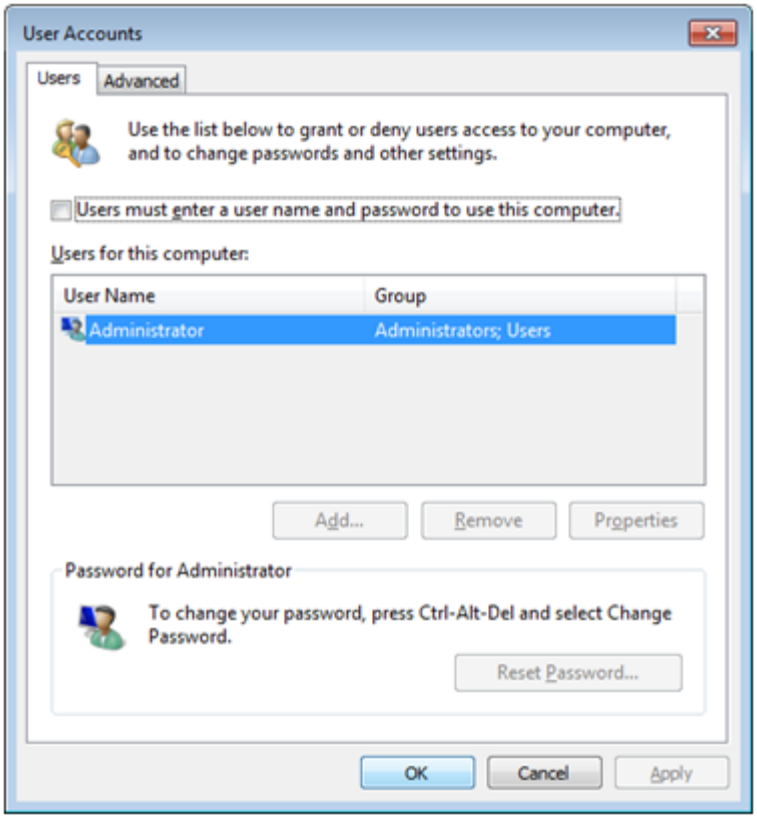


Figure 5-31 User Accounts window

29 Download Sigcheck on to the VM from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.

30 Extract sigcheck.zip to C:\WINDOWS\system32 location.

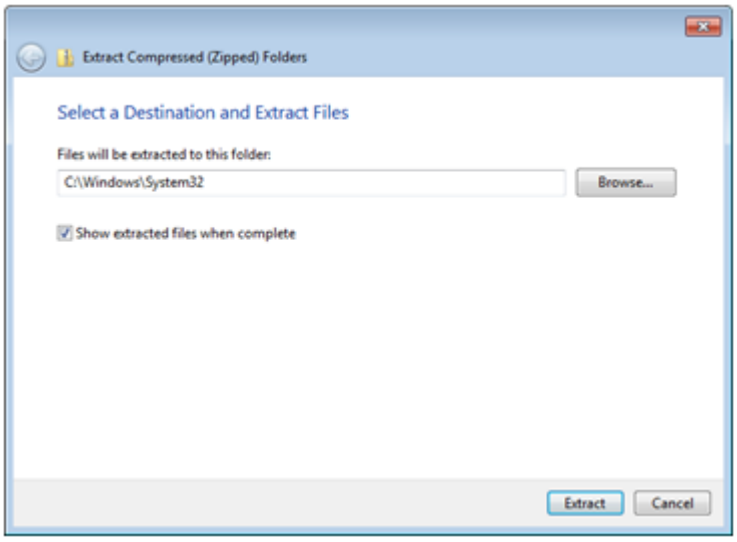


Figure 5-32 Extract the compressed folders

31 In Windows Explorer, go to C:\ WINDOWS\system32 and double-click **sigcheck.exe**.

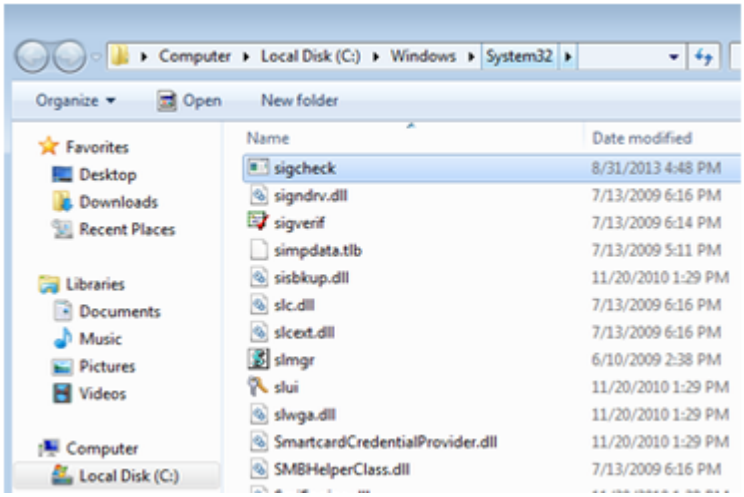


Figure 5-33 Run sigcheck.exe

32 If prompted, click **Run** in the warning message.

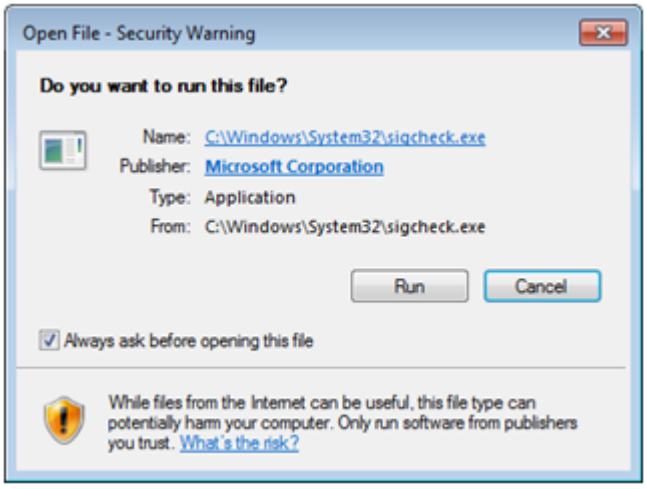
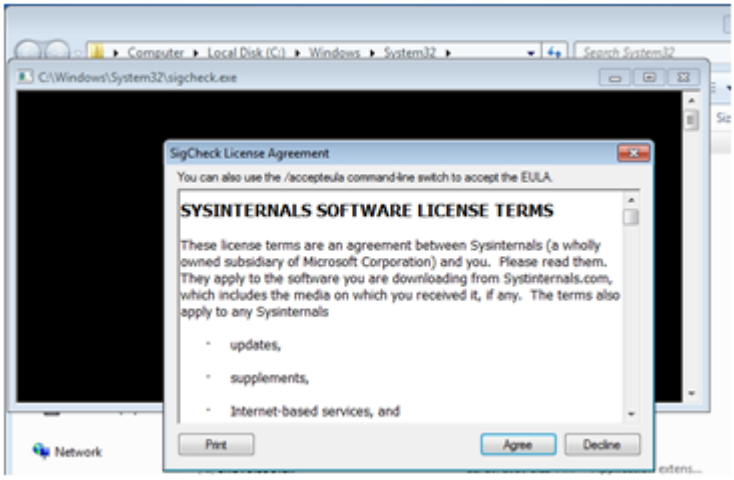

Open File - Security Warning
Do you want to run this file?
Name: C:\Windows\System32\sigcheck.exe
Publisher: Microsoft Corporation
Type: Application
From: C:\Windows\System32\sigcheck.exe
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Figure 5-34 Confirmation message

33 Click **Agree** for **Sigcheck License Agreement.**

Figure 5-35 Sigcheck license agreement


SigCheck License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline

34 Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip.

35 Extract MergeIDE.zip and run the MergeIDE batch file.

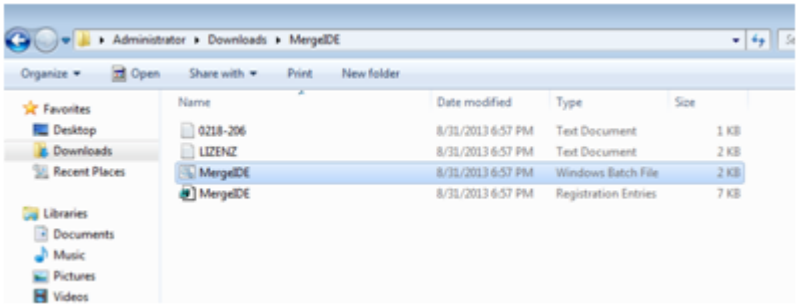


Figure 5-36 Run MergeIDE

36 If prompted, select **Run** in the warning message.

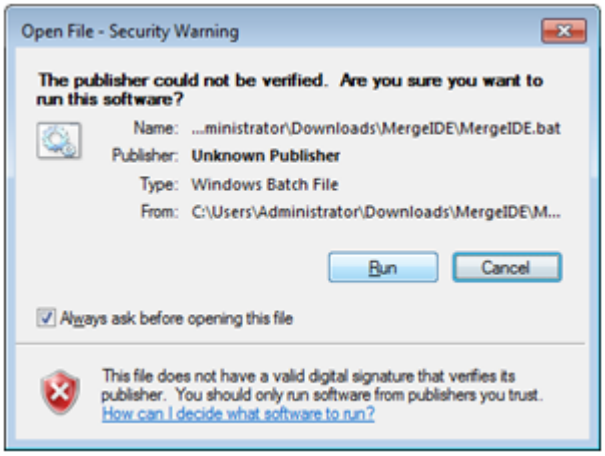

Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: ...ministrator\Downloads\MergeIDE\MergeIDE.bat
Publisher: Unknown Publisher
Type: Windows Batch File
From: C:\Users\Administrator\Downloads\MergeIDE\M...
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Figure 5-37 Warning message

37 Close Windows Explorer.

38 Verify if Windows is activated. Click **Start**, right-click **Computer**, then select **Properties**.

It is mandatory that Windows is activated.

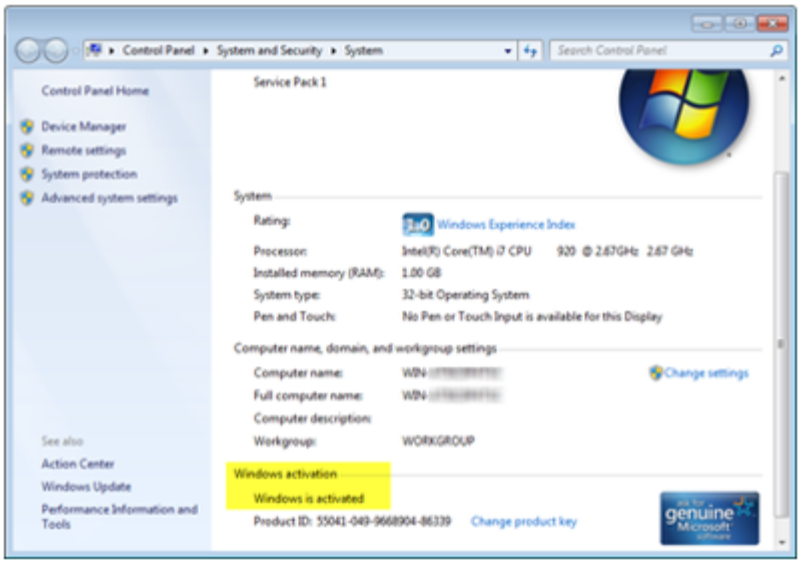


Figure 5-38 Activate Windows

39 Install a corresponding version of Microsoft Office on the virtual machine.

If you are installing an earlier version of Office, go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats to the virtual machine. You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open

a .docx file using Office 2003, you need the corresponding compatibility pack installed. After you download the compatibility pack, install it on the virtual machine.

a In VMware Workstation, right-click the virtual machine and select **Settings**.

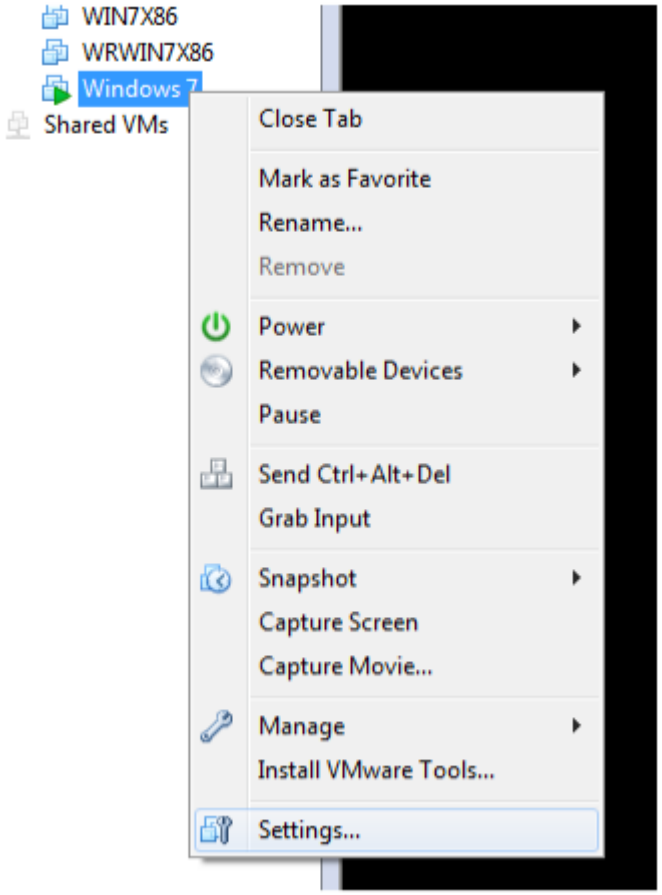


Figure 5-39 Settings option

b Select **CD/DVD (IDE)** and then select either **Use physical drive** or **Use ISO image file** and browse to the ISO image of Microsoft Office. Then click **OK**.

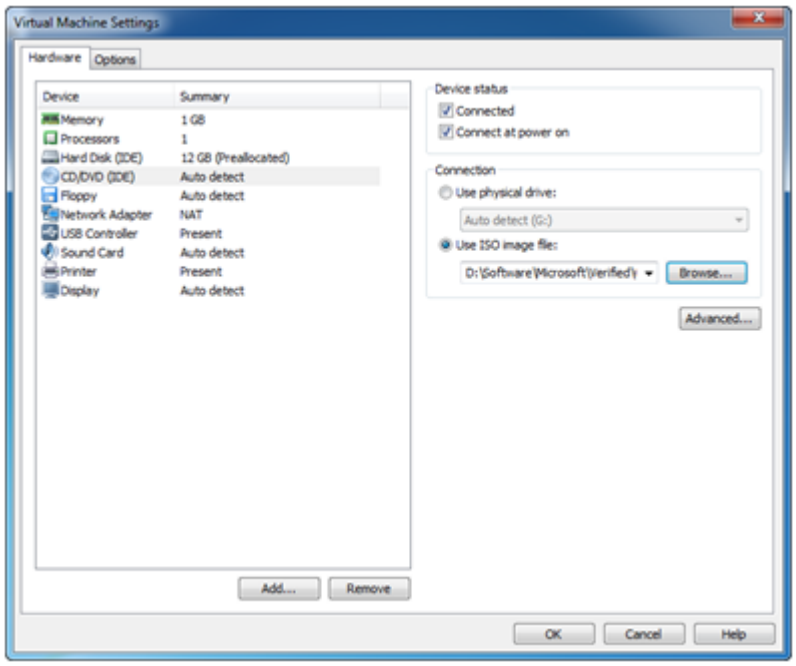


Figure 5-40 Browse to the ISO image of Microsoft Office

c After you enter the license key, select **Customize**.

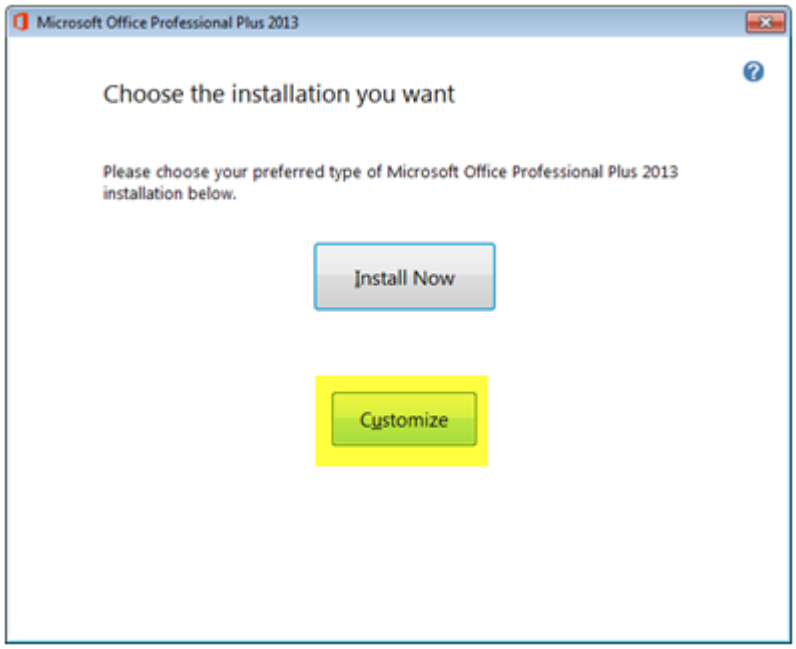

Microsoft Office Professional Plus 2013
Choose the installation you want
Please choose your preferred type of Microsoft Office Professional Plus 2013 installation below.
Install Now
Customize

Figure 5-41 Select to customize the installation

d Select **Run all from my computer** for Microsoft Office. Then select **Not Available** for applications such as Access, InfoPath, Lync, Outlook, Publisher, and Skydrive.

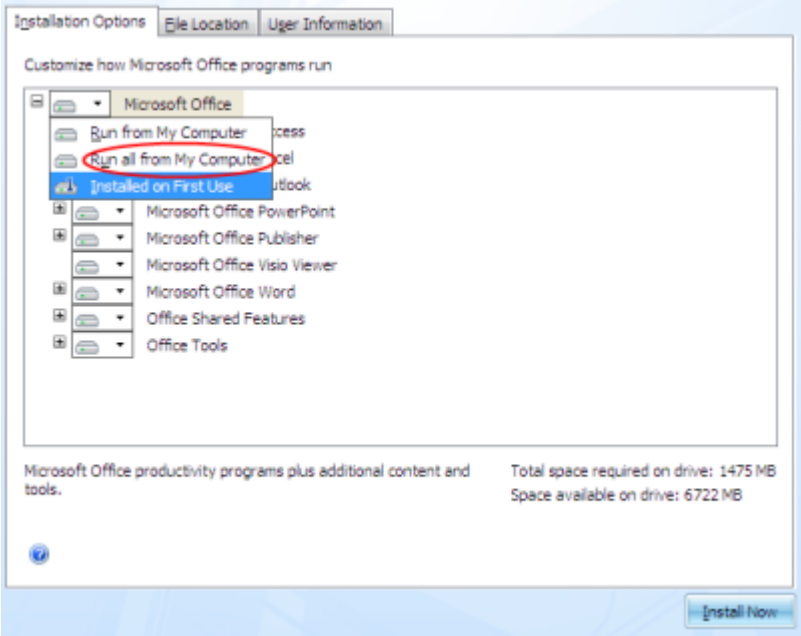


Figure 5-42 Specify the customization

40 To analyze PDF files, download Adobe Reader.

This procedure uses Adobe Reader 9.0 as an example.

a Install Adobe Reader 9.0.

b Open Adobe Reader and click **Accept**.

c In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates**.

41 For Windows XP, complete the following.

a Download Microsoft Visual C++ 2005 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=3387and install it.

b Download Microsoft Visual C++ 2008 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5582and install it.

c Download Microsoft Visual C++ 2010 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5555and install it.

d Download Microsoft .NET Framework 2.0 Service Pack 2 (x86 version) from http://www.microsoft.com/en-us/download/details.aspx?id=1639and install it.

42 To analyze JAR files, download and install Java Runtime Environment.

This procedure uses Java 7 Update 25 as an example.

a Open Java in the Control Panel.

b In the **Update** tab, deselect **Check for Updates Automatically.**

c In the Java Update Warning dialog, select **Do Not Check.**

d Click **OK** in the Java Control Panel.

43 In the Windows Run dialog, enter msconfig.

44 In the System Configuration utility, go to the **Startup** tab.

45 Deselect *reader_sl* and *jusched* and then click **OK**.

46 Restart the VM.

47 Install the other required applications such as Adobe Flash Player and the required browser.

If there are more than one browser installed, you can configure a default browser.

48 Open the default browser and set it up for malware analysis.

This procedure uses Internet Explorer as an example.

a Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** | **Pop-up Blocker** | **Turn on Pop-up Blocker**.

b Select **Tools** | **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.

c Go to the **Advanced** tab of the Internet Options and locate **Security**.

d Select **Allow active content to run in files on My Computer**.

e Click **OK**.

49 Shut down virtualMachineImage by selecting **Start** | **Shut down**.

50 Go to the location that you provided in step 8 to find the VMDK file named as virtualMachineImage -flat.vmdk

Import a VMDK file into McAfee Advanced Threat Defense

To create an analyzer VM, you must first import the corresponding VMDK file into McAfee Advanced Threat Defense. You must use SFTP to import the VMDK file.

Task

1 Open an FTP client that supports SFTP.

For example, you can use WinSCP or FileZilla.

2 Connect to the FTP server on McAfee Advanced Threat Defense using the following credentials.

- Host: IP address of McAfee Advanced Threat Defense.
- Username: atdadmin
- Password: atdadmin
- Port: 22

3 Upload the VMDK file from the local machine to McAfee Advanced Threat Defense.

Convert the VMDK file to an image file

Before you begin

- You have uploaded the VMDK file to McAfee Advanced Threat Defense.
- You have admin-user permissions in McAfee Advanced Threat Defense.

Task

1 In the McAfee Advanced Threat Defense web application, select **Manage** | **Image Management**.

2 In the **Image Management** page, select the VMDK file that you imported from the **VMDK Image** drop-down.

3 Select the corresponding operating system from the **Operating System** drop-down.

4 Click **Convert**.

The time taken for this conversion depends on the size of the VMDK file. For a 15 GB file, an ATD-3000 might take around five minutes.

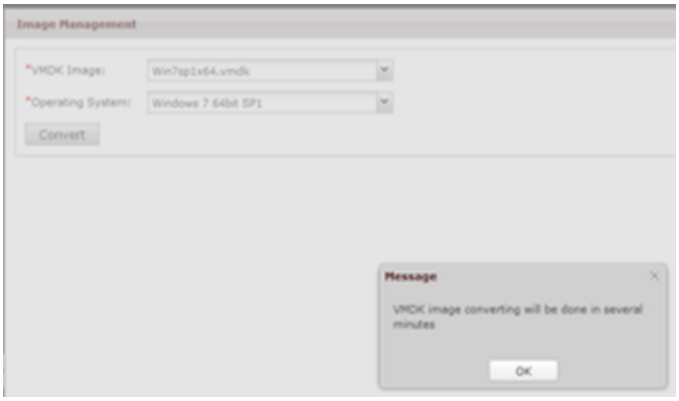


Figure 5-43 VMDK to image file conversion

After the conversion is complete, a message is displayed.

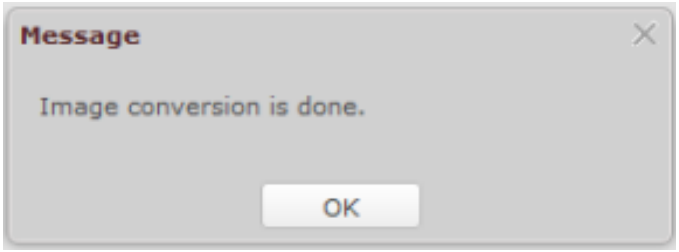


Figure 5-44 Confirmation message

Managing VM profiles

After you convert the imported VMDK file to an image file, you create a VM profile for that image file.

You cannot associate this VM profile with any other image file. Similarly, once associated, you cannot change the VM profile for an image file.

VM profiles contain the operating system and applications in an image file. This enables you to identify the images that you uploaded to McAfee Advanced Threat Defense and then use the appropriate image for dynamically analyzing a file. You can also specify the number of licenses that you possess for the operating system and the applications. McAfee Advanced Threat Defense factors this in when creating concurrent analyzer VMs from the corresponding image file.

You use the McAfee Advanced Threat Defense web application to manage VM profiles.

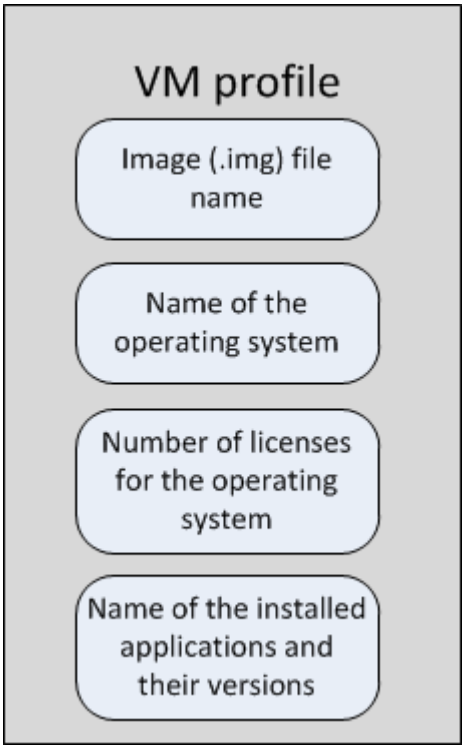

VM profile
Image (.img) file name
Name of the operating system
Number of licenses for the operating system
Name of the installed applications and their versions

Figure 5-45 Configurations in a VM profile

View VM profiles

You can view the existing VM profiles in the McAfee Advanced Threat Defense web application.

Task

1 Select **Policy | VM Profile**.

The currently available VM profiles are listed.

Column name	Definition
Select	Select to edit or delete the corresponding VM profile.
Name	Name that you have assigned to the VM profile.
Licenses	The number of end-user licenses that you possess for the corresponding operating system and applications. This is one of the factors that determine the number of concurrent analyzer VMs on McAfee Advanced Threat Defense.
Default	Whether this is a default VM profile.
Size	The size of the image file in megabytes.
Hash	The MD5 hash value of the image file.

2 Hide the unneeded columns.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

3 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific VM Profile, select the record and click **View**.

Create VM profiles

After you have converted the imported VMDK file to the image format, you can initiate the VM creation and also create the corresponding VM profile.

Each VMDK file that you imported must be associated with only one VM profile, which you cannot modify.

Task

1 Select **Policy** | **VM Profile** | **New.**.

The **VM Profile** page is displayed.

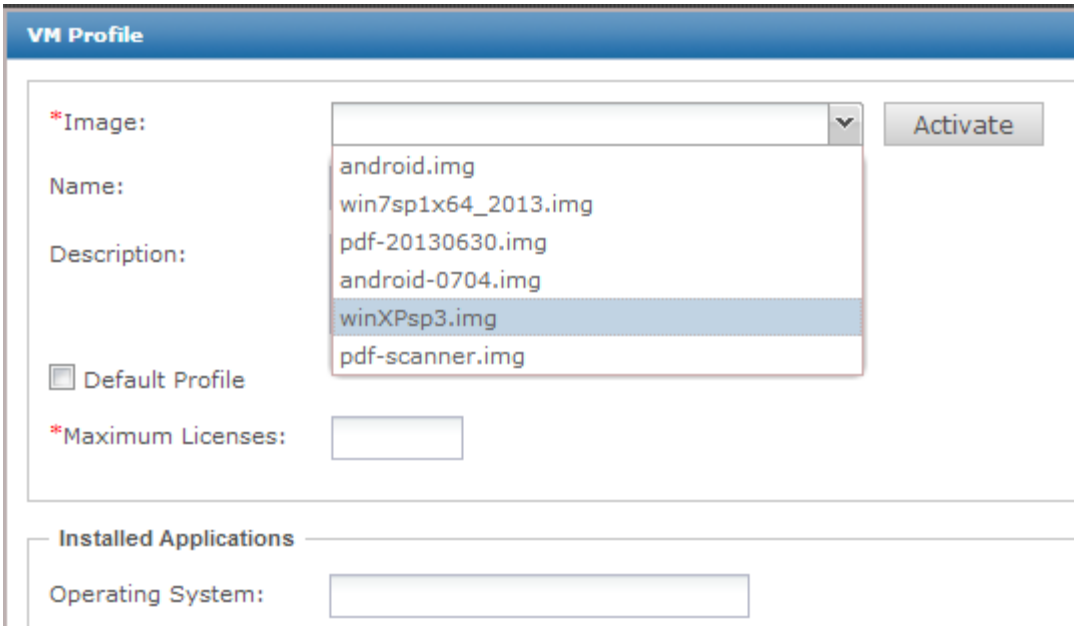


Figure 5-46 Select the image file

2 From the **Image** drop-down, select the one for which you want to create the VM profile.

3 Click **Activate** to create and activate the VM from the selected image file.

When you click **Activate**, the VM is opened in a pop-up window. So, make sure pop-up blocker is not enabled on your browser.

A progress bar indicating the VM creation is displayed.

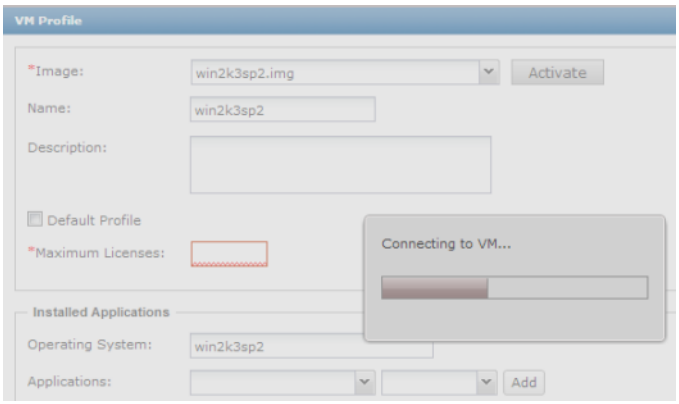


Figure 5-47 Progress of the VM creation

Based on your browser settings, warning messages are displayed before the VM starts.

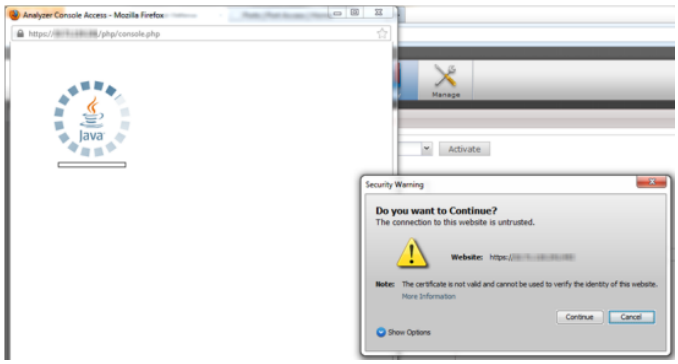


Figure 5-48 Warning message

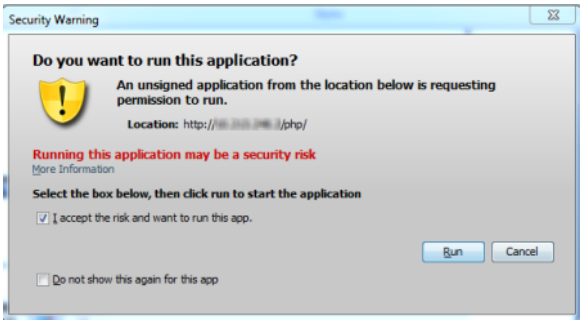

Security Warning
Do you want to run this application?
An unsigned application from the location below is requesting permission to run.
Location: http://
/php/
Running this application may be a security risk
More Information
Select the box below, then click run to start the application
I accept the risk and want to run this app.
Run
Cancel
Do not show this again for this app

Figure 5-49 Warning message

After you OK the warning messages, the VM starts.

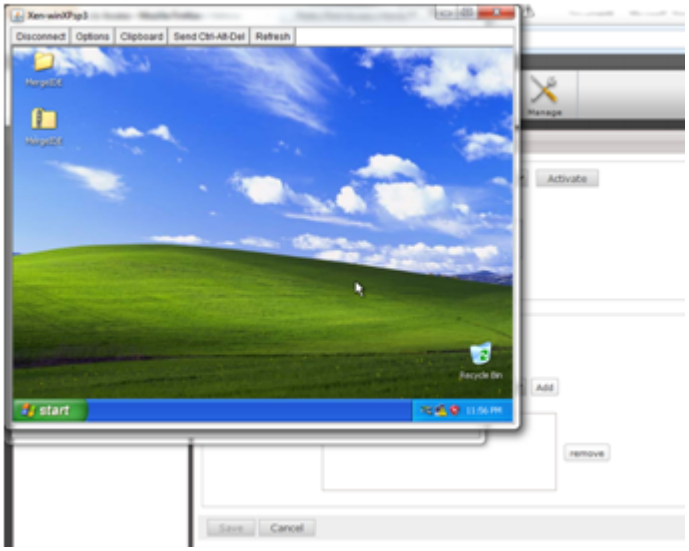


Figure 5-50 VM displayed in a pop-up window

4 Activate the VM, shut it down, and also close the pop-up window.

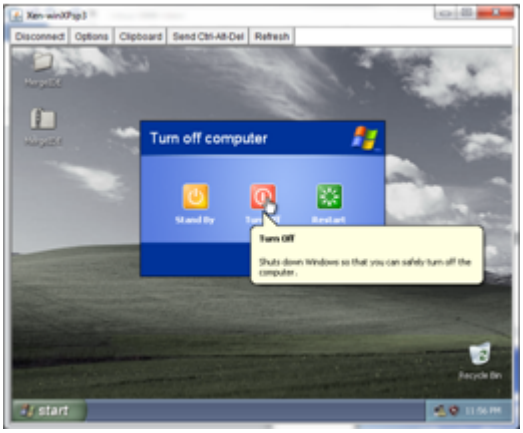


Figure 5-51 Shut down the VM

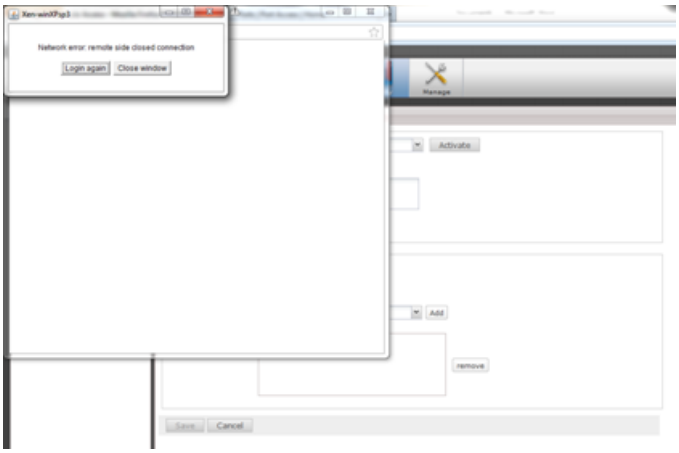


Figure 5-52 Close the pop-up window

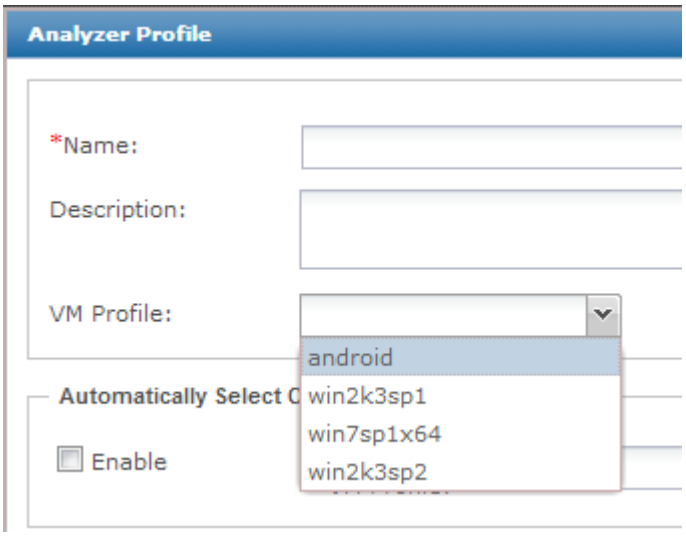
5 Create the VM profile for the VM that you created by entering the appropriate information in the respective fields.

Table 5-1 Option definitions

Option name	Definition
Name	The name of the image file is automatically displayed as the name for the VM profile. You cannot modify it.
Description	Optionally, provide a detailed description of the VM profile.
Default Profile	The first time, you must select it to make the VM profile the default one; subsequently you can select or ignore it. For a file, if the target host environment is not available or if the required analyzer VM is not available, McAfee Advanced Threat Defense uses this VM to dynamically analyze the file.
Maximum Licenses	Enter the number of concurrent user licenses that you possess. You must factor in the operating system as well as the applications in the image file. Consider that the image file is a Windows 7 machine with Microsoft Office installed. You have 3 concurrent licenses for Windows 7 and 2 for Microsoft Office. In this case, you must enter 2 as the maximum licenses. This is one of the factors that determine the number of concurrent analyzer VMs that McAfee Advanced Threat Defense creates from the image file.
Operating System	The name of the image file is automatically displayed as the name for the operating system. You cannot modify it.
Applications	Optionally, select the applications, such as browsers, Adobe PDF reader, and Microsoft Office contained in the image. You can also select the version for each application that you selected. This enables you to identify the contents of the image file.
Add	Click to include the application and version that you selected in the VM profile.
Remove	Select an added application and click **Remove** to remove it from the added applications list.
Save	Creates the VM profile record with the information you provided. When you click **Save**, the VM creation starts in the background, running as a daemon, and the VM profile is listed in the VM Profile page. Even if the newly created VM profile is listed in the **VM Profile** page, it might take 10-15 minutes before the analyzer VM and VM profile are ready for use.
Cancel	Closes the **VM Profile** page without saving the changes.

6 Select **Policy** | **Analyzer Profile** and check if the VM profile that you created is listed in the **VM Profile** drop-down.

Figure 5-53



Edit VM profiles

Before you begin

To edit a VM profile, either you must have created it or you must have admin-user role.

Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are listed.

2 Select the required record and click **Edit**.

The **VM Profile** page is displayed.

3 Make the changes to the required fields and click **Save**.

Delete VM profiles

Before you begin

- To delete a VM profile, either you must have created it or you must have admin-user role.
- Make sure the VM profile you want to delete is not specified in the analyzer profiles.

Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are displayed.

2 Select the required record and click **Delete**.

3 Click **Yes** to confirm deletion.

View the VM creation log

When you create a VM profile using the **VM Profile** page, McAfee Advanced Threat Defense creates an analyzer VM from the image file you selected in the VM profile record. Simultaneously, it prints the related logs, which you can view in the McAfee Advanced Threat Defense web application. Through these log entries, you can view what is happening as the analyzer VM is being created. You can use this information for troubleshooting purposes.

Task

- After you click **Save** in the **VM Profile** page, select **Manage** | **VM Creation Log** to view the log entries.

  You cannot print or export the log entries.

6 Configuring McAfee Advanced Threat Defense for malware analysis

After you install McAfee Advanced Threat Defense Appliance on your network, you can configure it to analyze malware. For this, you use the McAfee Advanced Threat Defense web application. You must have at least the web-access role to configure malware analysis.

This section introduces you to the related terminologies and provides the procedures to set up McAfee Advanced Threat Defense for malware analysis.

Contents

- *Terminologies*
- *High-level steps for configuring malware analysis*
- *How McAfee Advanced Threat Defense analyzes malware?*
- *Managing analyzer profiles*
- *Integration with McAfee ePO*
- *Specify proxy server for internet connectivity*
- *Configure the proxy DNS settings*

Terminologies

Being familiar with the following terminologies facilitates malware analysis using McAfee Advanced Threat Defense.

- **Static analysis** — When McAfee Advanced Threat Defense receives a supported file for analysis, it first performs static analysis of the file. The objective is to check if it is a known malware in the shortest possible time, and also to preserve the McAfee Advanced Threat Defense resources for dynamic

analysis. For static analysis, McAfee Advanced Threat Defense uses the following resources and in the same order:

- **Local whitelist —** This is the list of MD5 hash values of trusted files, which need not be analyzed. This whitelist is based on the McAfee® Application Control database that is used by other solutions in the McAfee suite. This has over 230,000,000 entries.

  The whitelist feature is enabled by default. To disable it, use the setwhitelist command. There are commands to manage the entries in the whitelist. The static McAfee® Application Control database cannot be modified. However, you can add or delete entries based on file hash. You can also query the whitelist for a certain file hash to see if it has been added to the database. The McAfee products that submit files to McAfee Advanced Threat Defense do have the capability to perform custom whitelisting as well. This includes the McAfee Web Gateway and the McAfee Network Security Platform

  See whitelist on page 137 for the commands.

- **Local blacklist —** This is the list of MD5 hash values of known malware stored in the McAfee Advanced Threat Defense database. When McAfee Advanced Threat Defense detects a malware through its heuristic McAfee Gateway Anti-Malware engine or through dynamic analysis, it updates the local blacklist with the file's MD5 hash value. A file is added to this list automatically only when its malware severity as determined by McAfee Advanced Threat Defense is medium, high, or very high. There are commands to manage the entries in the blacklist.

  See Blacklist on page 126 for the commands.

- **McAfee GTI —** This is a global threat correlation engine and intelligence base of global messaging and communication behavior, which enables the protection of the customers against both known and emerging electronic threats across all threat areas. The communication behavior includes the reputation, volume, and network traffic patterns. McAfee Advanced Threat Defense uses both the IP Reputation and File Reputation features of GTI.

- **Gateway Anti-Malware —** McAfee Gateway Anti-Malware Engine analyzes the behavior of web sites, web site code, and downloaded Web 2.0 content in real time to preemptively detect and block malicious web attacks. It protects businesses from modern blended attacks, including viruses, worms, adware, spyware, riskware, and other crimeware threats, without relying on virus signatures.

  McAfee Gateway Anti-Malware Engine is embedded within McAfee Advanced Threat Defense to provide real-time malware detection.

- **Anti-Malware** — McAfee Anti-Malware Engine is embedded within McAfee Advanced Threat Defense. The DAT is updated either manually or automatically based on the network connectivity of McAfee Advanced Threat Defense.

- **Dynamic analysis —** In this case, McAfee Advanced Threat Defense executes the file in a secure VM and monitors its behavior to check how malicious the file is. At the end of the analysis, it provides a detailed report as required by the user. McAfee Advanced Threat Defense does dynamic analysis after the static analysis is done. By default, if static analysis identifies the malware, McAfee Advanced Threat Defense does not perform dynamic analysis. However, you can configure McAfee Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis. You can also configure only dynamic analysis without static analysis. Dynamic analysis includes the disassembly listing feature of McAfee Advanced Threat Defense as well. This feature can generate the disassembly code of PE files for you to analyze the sample further.

- **Analyzer VM —** This is the virtual machine on the McAfee Advanced Threat Defense that is used for dynamic analysis. To create the analyzer VMs, you need to create the VMDK file with the required operating system and applications. Then, using SFTP, you import this file into the McAfee Advanced Threat Defense Appliance.

Only the following operating systems are supported to create the analyzer VMs:

- Windows XP SP2 32-bit
- Windows XP SP3 32-bit
- Windows Server 2003 SP1 32-bit
- Windows Server 2003 SP2 32-bit
- Windows Server 2008 64-bit
- Windows 7 SP1 32-bit
- Windows 7 SP1 64-bit
- Android

The only pre-installed analyzer VM is an Android 2.3 VM. You must create analyzer VMs for Windows. You can create different VMs based on your requirements. The number of analyzer VMs that you can create is limited only by the disk space of the McAfee Advanced Threat Defense Appliance. However, there is a limit as to how many of them can be used concurrently for analysis. The number of concurrent licenses that you specify also affects the number of concurrent instances for an analyzer VM.

- **VM profile —** After you upload the VM image (.vmdk file) to McAfee Advanced Threat Defense, you associate each of them with a separate VM profile. A VM profile indicates what is installed in a VM image and the number of concurrent licenses associated with that VM image. Using the VM image and the information in the VM profile, McAfee Advanced Threat Defense creates the corresponding number of analyzer VMs. For example, if you specify that you have 10 licenses for Windows XP SP2 32-bit, then McAfee Advanced Threat Defense understands that it can create up to 10 concurrent VMs using the corresponding .vmdk file.
- **Analyzer profile —** This defines how to analyze a file and what to report. In an analyzer profile, you configure the following:
  - VM profile
  - Analysis options
  - Reports you wish to see after the analysis
  - Password for zipped sample files
  - Minimum and maximum execution time for dynamic analysis

  You can create multiple analyzer profiles based on your requirements. For each McAfee Advanced Threat Defense user, you must specify a default analyzer profile. This is the analyzer profile that is used for all files uploaded by the user. Users who use the McAfee Advanced Threat Defense web application to manually upload files for analysis, can choose a different analyzer profile at the time of file upload. Always, the analyzer profile selected for a file takes precedence over the default analyzer profile of the corresponding user.

To dynamically analyze a file, the corresponding user must have the VM profile specified in the user's analyzer profile. This is how the user indicates the environment in which McAfee Advanced Threat Defense should execute the file. You can also specify a default Windows 32-bit and a 64-bit VM profile.

- **User —** A McAfee Advanced Threat Defense user is one who has the required permissions to submit files to McAfee Advanced Threat Defense for analysis and view the results. In case of manual submission, a user could use the McAfee Advanced Threat Defense web application or an FTP client. In case of automatic submission, you integrate McAfee products such as McAfee Network Security Platform or McAfee Web Gateway with McAfee Advanced Threat Defense. Then when these products detect a file download, they automatically submit the file to McAfee Advanced Threat Defense before allowing the download to complete. So, for these products default user profiles are available in McAfee Advanced Threat Defense.

  For each user, you define the default analyzer profile, which in turn can contain the VM profile. If you use the McAfee Advanced Threat Defense for uploading files for analysis, you can override this default profile at the time of file submission. For other users, McAfee Advanced Threat Defense uses the default profiles.

High-level steps for configuring malware analysis

This section provides the high-level steps on how to configure McAfee Advanced Threat Defense for malware analysis and reporting:

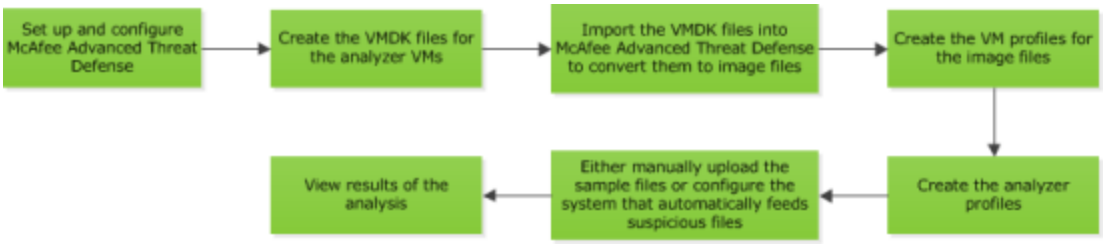

Set up and configure McAfee Advanced Threat Defense
Create the VMDK files for the analyzer VMs
Import the VMDK files into McAfee Advanced Threat Defense to convert them to image files
Create the VM profiles for the image files
Create the analyzer profiles
Either manually upload the sample files or configure the system that automatically feeds suspicious files
View results of the analysis

Figure 6-1 Summarized steps for configuring malware analysis

1. Set up the McAfee Advanced Threat Defense Appliance and ensure that it is up and running.
   - Based on your deployment option, make sure the McAfee Advanced Threat Defense Appliance has the required network connections. For example, if you integrate it with Network Security Platform, make sure the Sensor, Manager, and the McAfee Advanced Threat Defense Appliance are able to communicate with each other.
   - Make sure the required static analysis modules, such as the McAfee Gateway Anti-Malware Engine are up-to-date.
2. Create the analyzer VMs and the VM profiles. See Creating analyzer VM on page 4.
3. Create the analyzer profiles that you need. See Managing analyzer profiles on page 87.
4. If you want McAfee Advanced Threat Defense to upload the results to an FTP server, configure it and have the details with you before you create the profiles for the corresponding users.
5. Create the required user profiles. See Add users on page 35.
6. Log on to McAfee Advanced Threat Defense web application using the credentials of a user you created and upload a sample file for analysis. This is to check if you have configured McAfee Advanced Threat Defense as required. See Upload files for analysis using McAfee Advanced Threat Defense web application on page 97.

7 In the **Analysis Status** page, monitor the status of the analysis. See Monitor the status of malware analysis on page 100

8 After the analysis is complete, view the report in the **Analysis Results** page. See View the analysis results on page 102.

How McAfee Advanced Threat Defense analyzes malware?

This section explains a typical workflow when McAfee Advanced Threat Defense analyzes files for malware.

Consider that you have uploaded a file manually using McAfee Advanced Threat Defense web application:

1 Assuming the file format is supported, McAfee Advanced Threat Defense unpacks the file and calculates the MD5 hash value.

2 McAfee Advanced Threat Defense applies the analyzer profile that you specified during file upload.

3 Based on the configuration in the analyzer profile, it determines the modules to use for static analysis and checks the file against those modules.

4 If the file is found to be malicious during static analysis, McAfee Advanced Threat Defense stops further analysis and generates the required reports. This, however, depends on how you have configured the corresponding analyzer profile.

5 If the static analysis does not report any malware or if you had configured McAfee Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis, McAfee Advanced Threat Defense initiates dynamic analysis for the file.

6 It executes the file in the corresponding analyzer VMs and records every behavior. The analyzer VM is determined based on the VM profile in the analyzer profile.

7 If the file is fully executed or if the maximum execution period expires, McAfee Advanced Threat Defense prepares the required reports.

8 After dynamic analysis is complete, it sets the analyzer VMs to their baseline version so that they can be used for the next file in queue.

Managing analyzer profiles

When a file is manually or automatically submitted to McAfee Advanced Threat Defense for analysis, it uses the corresponding analyzer profile to determine how the file needs to be analyzed and what needs to be reported in the analysis results. You specify the VM profile in the analyzer profile. You also define how the file is to be analyzed for malware and the reports to be published. Thus, an analyzer profile contains all the critical user-configuration on how to analyze a file.

You use the McAfee Advanced Threat Defense web application to manage analyzer profiles.

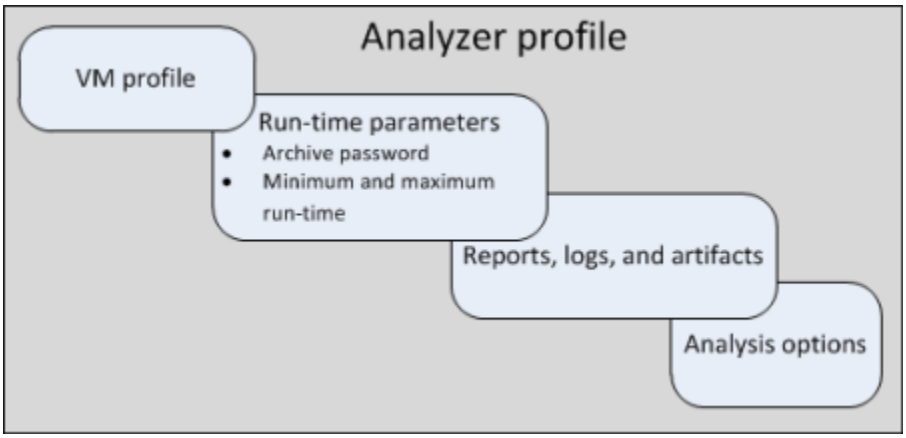


Figure 6-2 Contents of an analyzer profile

View analyzer profiles

Based on your user role, you can view the existing analyzer profiles in the McAfee Advanced Threat Defense web application.

Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

Column name	Definition
Select	Select to edit or delete the corresponding analyzer profile.
Name	Name that you have assigned to the analyzer profile.
Description	The description of the characteristics of the analyzer profile.
OS Name	Corresponds to the name of the VM profile specified in the analyzer profile.
Automatically Select OS	Indicates if you have selected the **Automatically Select OS** option in the analyzer profile.

2 Hide the unneeded columns.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

3 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific analyzer profile, select the record and click **View**.

Create analyzer profiles

Before you begin

If you intend to select the dynamic analysis option in the analyzer profile, make sure that you have created the required VM profile. VM profiles are also required if you want to use the **Automatically Select OS** option.

Task

1 Select **Policy** | **Analyzer Profile** | **New**.

The **Analyzer Profile** page is displayed.

2 Enter the appropriate information in the respective fields.

Option name	Definition
Name	Enter the name for the analyzer profile. It should allow you to easily identify the characteristics of that analyzer profile.
Description	Optionally, provide a detailed description of the analyzer profile.
VM Profile	Select the VM profile McAfee Advanced Threat Defense must use for dynamically analyzing a file.
Automatically Select OS	If you want McAfee Advanced Threat Defense to automatically select the VM profile for Windows 32 bit and Windows 64 bit, select **Enable** and then select the VM profiles from the **Windows 32-bit VM Profile** and **Windows 64-bit VM Profile**.
Archive Password	Enter the password for McAfee Advanced Threat Defense to unzip a password-protected malware sample.
Confirm Password	Re-enter the password for confirmation.
Minimum Run Time (sec)	Specify the minimum time duration for which McAfee Advanced Threat Defense should dynamically analyze the sample. The default value is 60 seconds. If the file stops executing before this time period, the dynamic analysis is stopped.
Maximum Run Time (sec)	Specify the maximum time duration for which McAfee Advanced Threat Defense should dynamically analyze the sample. If the file does not stop execution before this time period expires, the dynamic analysis is stopped.
Analysis Summary	Select to include the Analysis Summary report in the analysis results. See View the Analysis Summary report on page 104.
Packet captures	Select to capture the network packets if the file attempts to communicate during dynamic analysis.
Dropped Files	Select to generate the Files Created in Sandbox report. See Dropped files report on page 110.
Disassembly Results	Select if you want McAfee Advanced Threat Defense to generate the disassembly code of PE files. See Disassembly Results on page 110.
Execution Path Data	Select to generate Execution Path Listing report. See Logic Path Graph on page 111.
User API Log	This report provides Windows user-level DLL API calls made directly by the malware sample during dynamic analysis. See User API Log on page 116.
Local Black List	Select if you want McAfee Advanced Threat Defense to check the file's MD5 hash value with the list of black-listed MD5 hash values in its local database.
Anti-Malware	Select if you want McAfee Advanced Threat Defense to scan the file using McAfee Anti-Malware Engine.
GTI File Reputation	Select if you want McAfee Advanced Threat Defense to check the file's MD5 hash value with McAfee GTI. Make sure McAfee Advanced Threat Defense is able to communicate with McAfee GTI, which is on the cloud.
Gateway Anti-Malware	Select if you want McAfee Advanced Threat Defense to check the file using McAfee Gateway Anti-Malware Engine.
Sandbox	Select if you want the file to be dynamically analyzed. A file is not dynamically analyzed if any of the static methods report it as a malware or a white-listed file. If you want to dynamically analyze the file regardless of the result from static analysis, select **Run All Selected** as well. Make sure you have selected the VM profile and the **Runtime Parameters**.
Run All Selected	Select if you want McAfee Advanced Threat Defense to analyze the file using all the selected analyze options regardless of the result from any specific method.

Option name	Definition
Save	Creates the analyzer profile record with the information you provided.
Cancel	Closes the **Analyzer Profile** page without saving the changes.

Edit analyzer profiles

Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2 Select the required record and click **Edit**.

The **Analyzer Profile** page is displayed.

3 Make the changes to the required fields and click **Save**.

The changes affect the corresponding users even if they are currently logged on.

Delete analyzer profiles

Before you begin

Make sure the users to whom you have assigned this analyzer profile are not currently logged on to McAfee Advanced Threat Defense.

Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2 Select the required record and click **Delete**.

3 Click **Yes** to confirm deletion.

Integration with McAfee ePO

Integrating McAfee Advanced Threat Defense and McAfee ePO enables McAfee Advanced Threat Defense to correctly identify the target host environment and use the corresponding analyzer VM for dynamic analysis.

For McAfee Advanced Threat Defense to query McAfee ePO for host information, you must install Real Time for ePolicy Orchestrator®. However, McAfee Advanced Threat Defense queries only McAfee ePO. This in turn queries Real Time for ePolicy Orchestrator® (Real Time for McAfee ePO™) for host information.

To determine the analyzer VM for a file submitted by Network Security Platform or McAfee Web Gateway, McAfee Advanced Threat Defense uses the following sources of information in the same order of priority:

1. McAfee Advanced Threat Defense queries McAfee ePO for the operating system of a host based on its IP address. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
2. If Device Profiling is enabled, the Sensor provides the operating system and application details when forwarding a file for analysis. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
3. From the analyzer profile in the corresponding user record, McAfee Advanced Threat Defense determines the VM profile. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
4. The VM profile that you selected as the default. From the VM profiles in your setup, you can select one of them as the default one.

When McAfee Advanced Threat Defense receives host information for a particular IP address from McAfee ePO, it caches this detail.

- The cached IP address to host information data has a time to live (TTL) value of 48 hours.
- For the first 24 hours, McAfee Advanced Threat Defense just uses the host information in the cache.
- For the second 24 hours, that is from 24 to 48 hours, McAfee Advanced Threat Defense uses the host information from the cache but also queries McAfee ePO and updates its cache. This updated information is valid for the next 48 hours.
- If the cached information is more than 48 hours old, it treats it as if there is no cached information for the corresponding IP address. That is, it attempts to find the information from other sources and also sends a query to McAfee ePO.

The following explains how McAfee Advanced Threat Defense collaborates with McAfee ePO.

1. Network Security Platform or McAfee Web Gateway sends a file to McAfee Advanced Threat Defense for analysis. When Network Security Platform sends a file, the IP address of the target host is also sent.
2. McAfee Advanced Threat Defense checks its cache to see if there is a valid operating system mapped to that IP address.
3. If it is the first time that a file for that IP address is being analyzed, there is no information in the cache. So, it determines the analyzer VM from the device profiling information in case of Network Security Platform and user record in case of McAfee Web Gateway. Simultaneously, it sends a query to McAfee ePO for host information based on the IP address.
4. McAfee ePO then queries Real Time for ePolicy Orchestrator® (Real Time for McAfee ePO™) for host information.
5. McAfee ePO then forwards the host information to McAfee Advanced Threat Defense, which is cached for further use.

Configure McAfee ePO integration

Integration with McAfee ePO, enables McAfee ePO to gather information such as the operating system and browsers installed on the target host. McAfee Advanced Threat Defense uses this information to select the best analyzer VM for dynamic analysis.

Task

1 Select **Manage** | **ePO Login**.

The **ePO Login** page displays.

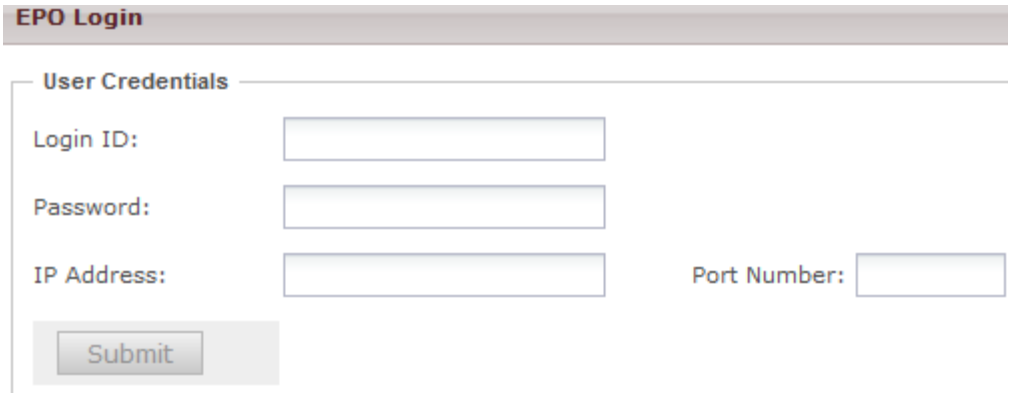


Figure 6-3 McAfee ePO integration

2 Enter the details in the appropriate fields.

Option name	Definition
Login ID	Enter the McAfee ePO login name that McAfee Advanced Threat Defense should use to access the McAfee ePO server. McAfee recommends you create a McAfee ePO user account with View-only permissions required for integration.
Password	Enter the password corresponding to the **Login ID** you entered.
IP Address	Enter the IPv4 address of the McAfee ePO server. Contact your McAfee ePO administrator for the IP address.
Port Number	Specify the HTTPS listening port on the McAfee ePO server that will be used for the McAfee Advanced Threat Defense — McAfee ePO communication. Contact your McAfee ePO administrator for the port number.
Submit	Click to save the configuration and enable McAfee Advanced Threat Defense — McAfee ePO integration.

Specify proxy server for internet connectivity

If McAfee Advanced Threat Defense connects to a proxy server for internet connectivity, you can configure McAfee Advanced Threat Defense to connect to that server for proxy service.

Task

1 Select **Manage** | **HTTP Proxy Setting**.

The **HTTP Proxy Setting** page is displayed.

Figure 6-4 Proxy Setting **page**

2 Enter the appropriate information in the respective fields.

Option name	Definition
Enable Proxy	Select to connect McAfee Advanced Threat Defense to a proxy server for Internet connectivity.
User Name	Enter the user name that McAfee Advanced Threat Defense for the proxied Internet connection.
Password	Enter the corresponding password.
Proxy IP Address	Enter the IPv4 address of the proxy server.
Port Number	Enter the port number on which the proxy server is listening for incoming connections.
Submit	Click to save the proxy settings in the database.

Configure the proxy DNS settings

When being executed, some files might send DNS queries to resolve names. Mostly, such queries are an attempt by malware to determine if they are being run in a sandbox environment. If the DNS query fails, the file might take an alternate path. When McAfee Advanced Threat Defense dynamically analyzes such a file, you might want to provide a proxy DNS service in order to bring out the actual behavior of the file.

Task

1 Select **Manage** | **DNS Proxy Setting**.

The **DNS Proxy Setting** page is displayed.

2 Enter the appropriate information in the respective fields.

Option name	Definition
Domain	Enter the Active Directory domain name, for example, McAfee.com.
Preferred DNS Server	Enter the IPv4 address of the primary DNS proxy server. The DNS queries from analyzer VMs are come to this DNS server.
Alternate DNS Server	Enter the IPv4 address of the secondary DNS proxy server. If the analyzer VM is unable to reach the primary DNS server, the DNS queries come to the secondary DNS server.
Submit	Click to save the configuration in the database.

7 Analyzing malware

After you have configured McAfee Advanced Threat Defense, you can upload files for analysis. The following are the methods you can follow to submit files:

- Manually upload the file using the McAfee Advanced Threat Defense web application.
- Post the file on the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Use the restful APIs of McAfee Advanced Threat Defense web application to upload the file. See the *McAfee Advanced Threat Defense RESTful APIs Reference Guide.*
- Integrate McAfee Advanced Threat Defense with Network Security Platform and McAfee Web Gateway. Then, these applications automatically submit samples to McAfee Advanced Threat Defense. See the corresponding documentation.

You can monitor the status of malware analysis using McAfee Advanced Threat Defense web application and then view the results.

Contents

- *Upload files for analysis using McAfee Advanced Threat Defense web application*
- *Upload files for analysis using SFTP*
- *Monitor the status of malware analysis*
- *View the analysis results*
- *Working with the McAfee Advanced Threat Defense Dashboard*

Upload files for analysis using McAfee Advanced Threat Defense web application

Before you begin

The required analyzer profile is available.

When you use the McAfee Advanced Threat Defense web application to submit a file for analysis, you must select an analyzer profile. This analyzer profile overrides the default analyzer profile associated with your user account.

Task

1 Select **Analysis** | **Manual Upload.**

2 In the **Manual Upload** page, specify the details as per your requirement.

Table 7-1 Option definitions

Option	Definition
File	Either drag and drop the malware file from Windows Explorer or click **Browse** and select the file. If you want to submit multiple files, upload them in a .zip file. • If you are uploading a password-protected .zip file, make sure you have provided the password in the analyzer profile that you want to use for analysis. • If dynamic analysis is required, the files in the .zip file are executed on different instances of the analyzer VM. If enough analyzer VMs are not available, some of the files are in pipeline until analyzer VMs are available. • Because the files in the .zip file are analyzed separately, separate reports are created for each file.
Analyzer Profile	Select the required analyzer profile for the sample.
Advanced	Click to specify additional parameters for analyzing the sample. The **Advanced** options are available only when you manually submit the file using McAfee Advanced Threat Defense web application. • **Region:** In some cases, the behavior of a file might vary based on the geographical location of the target system. For example, malware from a rogue nation might not cause any harm to computers in its own country or that of its friends. Select the country if you want to analyze the malware in relation to location. You cannot modify the list of countries. This list might be updated when you upgrade McAfee Advanced Threat Defense software. • **User Interactive Mode:** Upon execution, some malware require user input. This is typically done to check if the malware is being analyzed in a sandbox. In the absence of user input, the malware might take an alternative execution path or even might suspend further execution. If you select this option, you can access the actual analyzer VM on which the malware is executed and provide the required input. See Upload files for analysis in user-interactive mode on page 98. After you made the required selections, click **OK**.
Submit	Click to upload the file to McAfee Advanced Threat Defense for analysis.

Tasks

- *Upload files for analysis in user-interactive mode* on page 98

Upload files for analysis in user-interactive mode

Before you begin

You have created the required analyzer profile that you want to use.

When being executed, some files might open dialog boxes, where you might be required to make a selection. Malware demonstrates such behavior to determine if they are being executed in a sandbox. The behavior of the malware might vary based on your intervention. When you submit files in this mode, the analyzer VM is opened in a pop-up window on your client computer and you can make the required selections when prompted

You can upload files to be executed in the user-interactive mode. This option is available only when you manually upload a file using the McAfee Advanced Threat Defense web application. For files submitted by other methods, such as FTP upload and files submitted by Network Security Platform,

requests for user-intervention by the malware are not honored. However, the screen shots of all such requirements are available in the **Screenshots** section of the **Analysis Summary** report. Then you can manually resubmit such files in the user-interactive mode to know the actual behavior of the file.

This section uses an example to show how files are analyzed in user-interactive mode.

Task

1 Select **Analysis** | **Upload File**.

2 In the **Upload File** field, click **Browse** and select the file you want to submit for analysis.

3 In the **Analyzer Profile** field, select the required analyzer profile from the drop-down list.

4 Click **Advance** and select **User Interactive Mode**.

5 Click **OK** and then **Submit**.

A pop-up window opens in your machine. Security warnings might be displayed based on your browser settings. After you confirm the security warnings, the analyzer VM is displayed in the pop-up window and the dialog boxes opened by the sample are displayed.

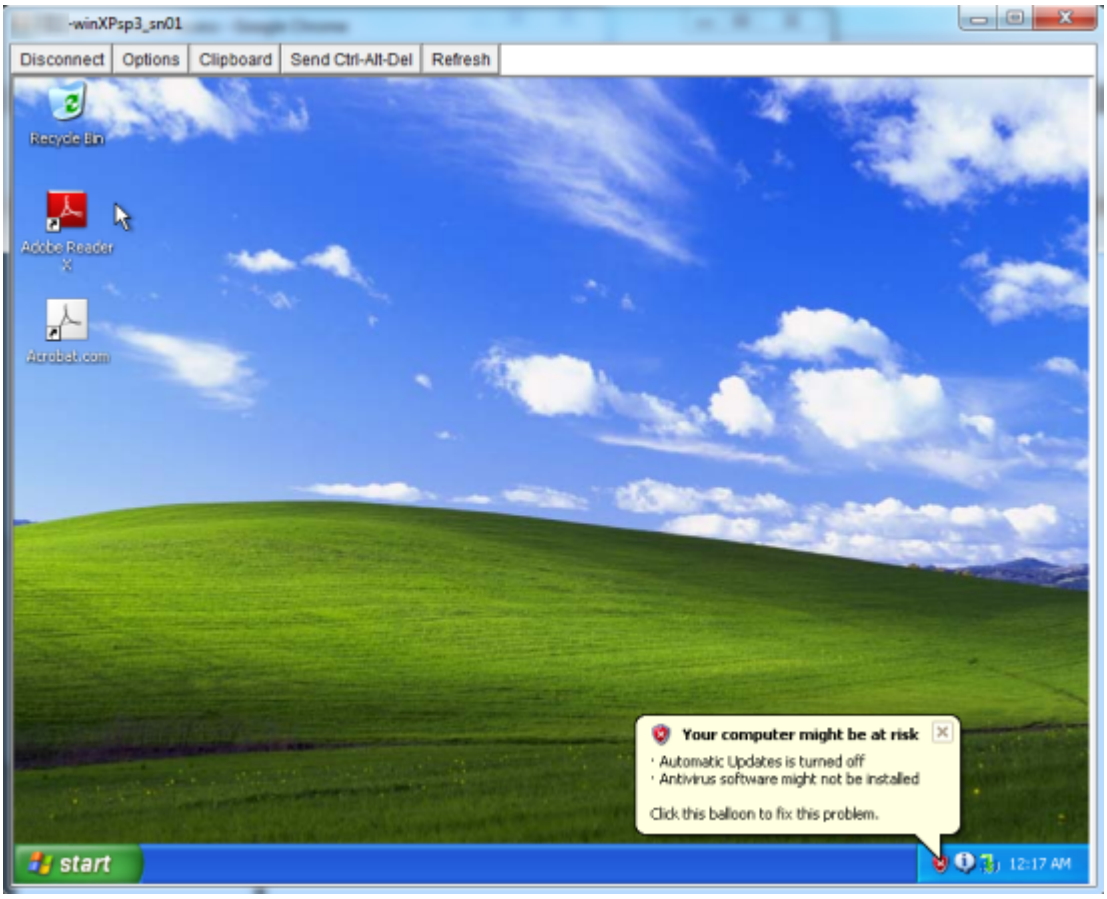


Figure 7-1 Analyzer VM accessible in a pop-up window

You can use your mouse and keyboard to provide your input. After the file completes execution, click **Disconnect** to close the analyzer VM.

Upload files for analysis using SFTP

Before you begin

- Your user name has **FTP Access** privilege. This is required to access the FTP server hosted on McAfee Advanced Threat Defense.
- You have created the required analyzer profile that you want to use.
- You have installed an FTP client on your machine.

Using SFTP, you can upload the supported file types to the FTP server on McAfee Advanced Threat Defense. FTP is not a supported protocol for uploading samples.

Task

1 Open your FTP client and connect to McAfee Advanced Threat Defense using the following information.
   - Host — Enter the IP address of McAfee Advanced Threat Defense.
   - User name — Enter your McAfee Advanced Threat Defense user name.
   - Password — Enter your McAfee Advanced Threat Defense password.
   - Port — Enter 22, which is the standard port for SFTP.

2 Upload the files from the local site to the remote site, which is on McAfee Advanced Threat Defense.

3 In the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Status** to monitor the status of the uploaded files.

Monitor the status of malware analysis

After you submit a file for analysis, you can monitor the status from the **Analysis Status** page.

Task

1 Select **Analysis** | **Analysis Status**.

The **Analysis Status** page lists the status for the submitted files.

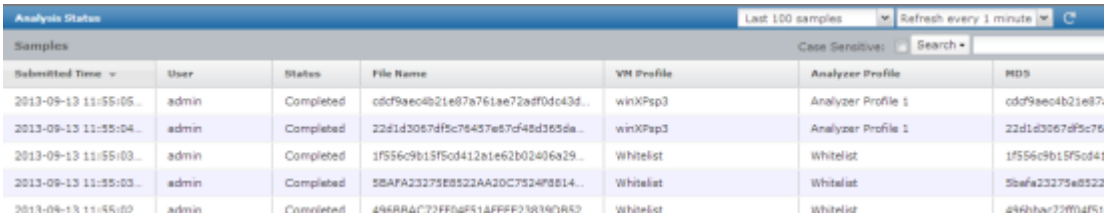


Figure 7-2 Status of files submitted for analysis

If you do not have admin permissions, only those files that you submitted are listed. A user with admin permissions can view the samples provided by any user.

2 Specify the criteria for viewing and refreshing the status of files being analyzed.

   a Set the criteria to display records in the **Analysis Status** page.

   You can specify this criteria based on time or number. For example, you can select to view the status for files submitted in the last 5 minutes or for the last 100 samples.

b Set the frequency at which the **Analysis Status** page must refresh itself.

The default refresh interval is 1 minute.

c To refresh the **Analysis Status** page now, click .

3

4 Filter the displayed records to locate the required ones.

Table 7-3 Filtering options

Option	Definition
Search	Specify the parameter that you want to use to filter the records. Click **Search** and select one or more of the following parameters: • **File Name**: Select if you want to filter based on the starting characters of the file name. For example, if you select this option and enter *cal* as the search string then the status for files names that start with *cal* are listed. • **MD5**: Select if you want to filter based on the starting characters of the MD5 hash value. • **Status**: Select if you want to filter based on the status - Waiting, Analyzing, or Completed. Enter the search string in the adjacent text box.
Case Sensitive	Select if you want to make the search case sensitive.

Suppose that you have selected **File Name** and **Status** as the criteria, selected **Case Sensitive**, and specified *Com*. All the records in the completed state and file names starting with the characters *Com* are listed.

Table 7-4 Column definitions

Column	Definition
Submitted Time	The time stamp when the file was submitted for analysis.
User	The log on name of the user who submitted the file for analysis.
Status	The current status of analysis. • **Waiting —** Typically, this indicates that McAfee Advanced Threat Defense is waiting for an analyzer VM to dynamically analyze the file. • **Analyzing —** Indicates that the analysis is still in progress. • **Completed —** Indicates that the analysis is complete for the file. Double-click the record to see the complete report.
File Name	The name of the file that you submitted for analysis.
VM Profile	The VM profile used for dynamic analysis. If the file was analyzed only by a static method, that is displayed.
Analyzer Profile	The analyzer profile that was referred to for the analysis. If the file was analyzed only by a static method, that is displayed.
MD5	The MD5 hash value of the file as calculated by McAfee Advanced Threat Defense.
File Type	The file type of the sample, such as binary.

5 Hide the columns that you do not require.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

6 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

View the analysis results

After you submit a file for analysis, you can view the results in the **Analysis Results** page.

Task

1 Select **Analysis** | **Analysis Results**.

The **Analysis Results** page lists the status for the completed files.

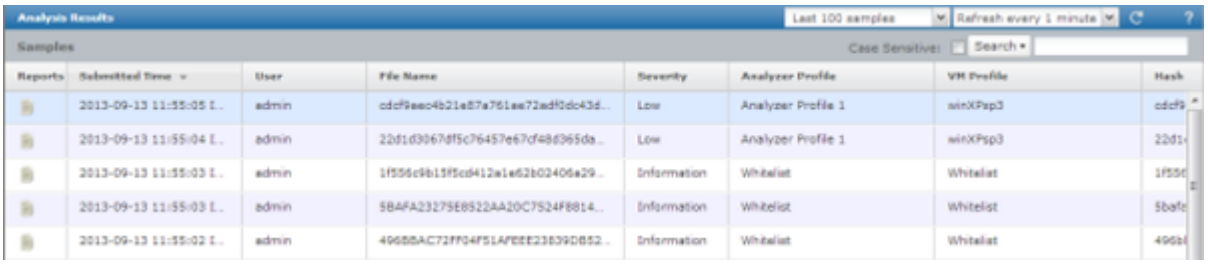


Figure 7-3 Status of files submitted for analysis

If you do not have admin permissions, only those files that you submitted are listed. A user with admin permissions can view the samples submitted by all users.

2 Specify the criteria for viewing and refreshing the records in the **Analysis Results** page.

a Set the criteria to display records in the **Analysis Results** page.

You can specify this criteria based on time or number. For example, you can select to view the files for which the analysis was completed in the last 5 minutes or for the last 100 completed files.

b Set the frequency at which the **Analysis Results** page must refresh itself.

The default refresh interval is 1 minute.

c To refresh the **Analysis Results** page now, click .

Table 7-5 Column definitions

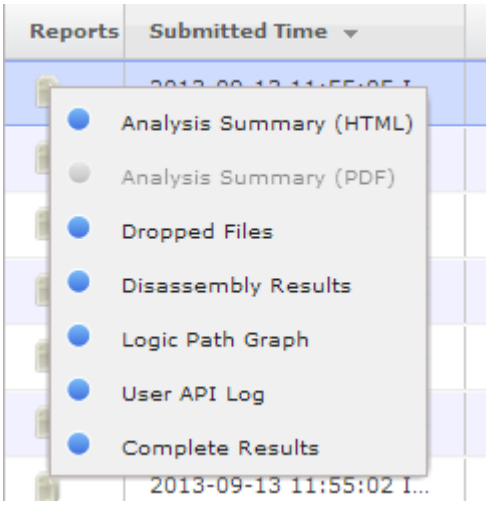
Column	Definition
Reports	Click to display the types of reports available for the sample.  Click any of the enabled reports to view the corresponding details. A specific report is enabled only if it is relevant to the analyzed file and also selected in the corresponding analyzer profile. • **Analysis Summary (HTML)** — This is the comprehensive report that is available for all file types. This report is also displayed when you double-click a record. • **Analysis Summary (PDF)** — Select this to view the report in PDF. • **Dropped Files** — Select this report to view the files that the analyzed sample created during dynamic analysis. • **Disassembly Results** — Select this to view the assembly language code reverse-engineered from the file. This report is relevant only for sample types such as .exe and .dll. • **Logic Path Graph** — Select this to view a graphical representation of which subroutines were executed during the dynamic analysis and which were not. • **Dynamic Execution Logs** — Select this to view the Windows user-level DLL API calls made directly by the sample during dynamic analysis. • **Complete Results** — Click to download the .zip file containing all the report types to your local machine.
Submitted Time	The time stamp when the file was submitted for analysis.
User	The log on name of the user who submitted the file for analysis.

Table 7-5 Column definitions *(continued)*

Column	Definition
Severity	Indicates the severity level of the analyzed sample. • Information — Indicates that this is a clean file. White-listed files have this severity level. Corresponds to a severity score of zero. • Very low — Corresponds to a severity score of 1. • Low — Corresponds to a severity score of 2. • Medium — Corresponds to a severity score of 3. • High — Corresponds to a severity score of 4. • Very high — Corresponds to a severity score of 5.
File Name	The name of the file that you submitted for analysis.
Analyzer Profile	The analyzer profile that was referred to for the analysis.
VM Profile	The VM profile used for the dynamic analysis. If only static was used, that is displayed.
Hash	The MD5 hash value of the file as calculated by McAfee Advanced Threat Defense.
File Size	The size of the analyzed file in KB.

3 Choose to hide the columns that you do not require.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

4 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

View the Analysis Summary report

The Analysis Summary report is an executive brief detailing key behaviors of the sample file. This report is available in HTML, text, PDF, XML, and JSON formats.

The HTML, text, and PDF formats are mainly for you to review the analysis report. You can access the HTML and PDF formats from the McAfee Advanced Threat Defense web application. The HTML and text formats are also available in the reports .zip file for the sample, which you can download to your client computer.

The XML and JSON formats provide well-known malware behavior tags for high-level programming script to extract key information. Network Security Platform and McAfee Web Gateway use the JSON formats to display the report details in their user interfaces.

Task

1 To access the Analysis Summary report in the McAfee Advanced Threat Defense web application, do the following:

   a Select **Analysis** | **Analysis Results**.

   b To view the HTML format of the report, click and then select **Analysis Summary (HTML)**.

   Alternatively, you can double-click the required record.

   c To view the PDF of the report, click and then select **Analysis Summary (PDF)**.

2 To access the Analysis Summary report from the reports .zip file, do the following:

   a Select **Analysis** | **Analysis Results**.

   b Click and select **Complete Results**.

   c Save the zipped reports on your local machine.

   The .zip file is named after the name of the sample file.

   d Extract the contents of the .zip file.

   The AnalysisLog folder contains the HTML, text, XML, and JSON formats of the Analysis Report. You can identify these files by the malware file name. The malware file name is appended to _summary.html, _summary.json, _summary.txt, and _summary.xml.

The various sections of the HTML format of the Analysis Summary report are outlined here.

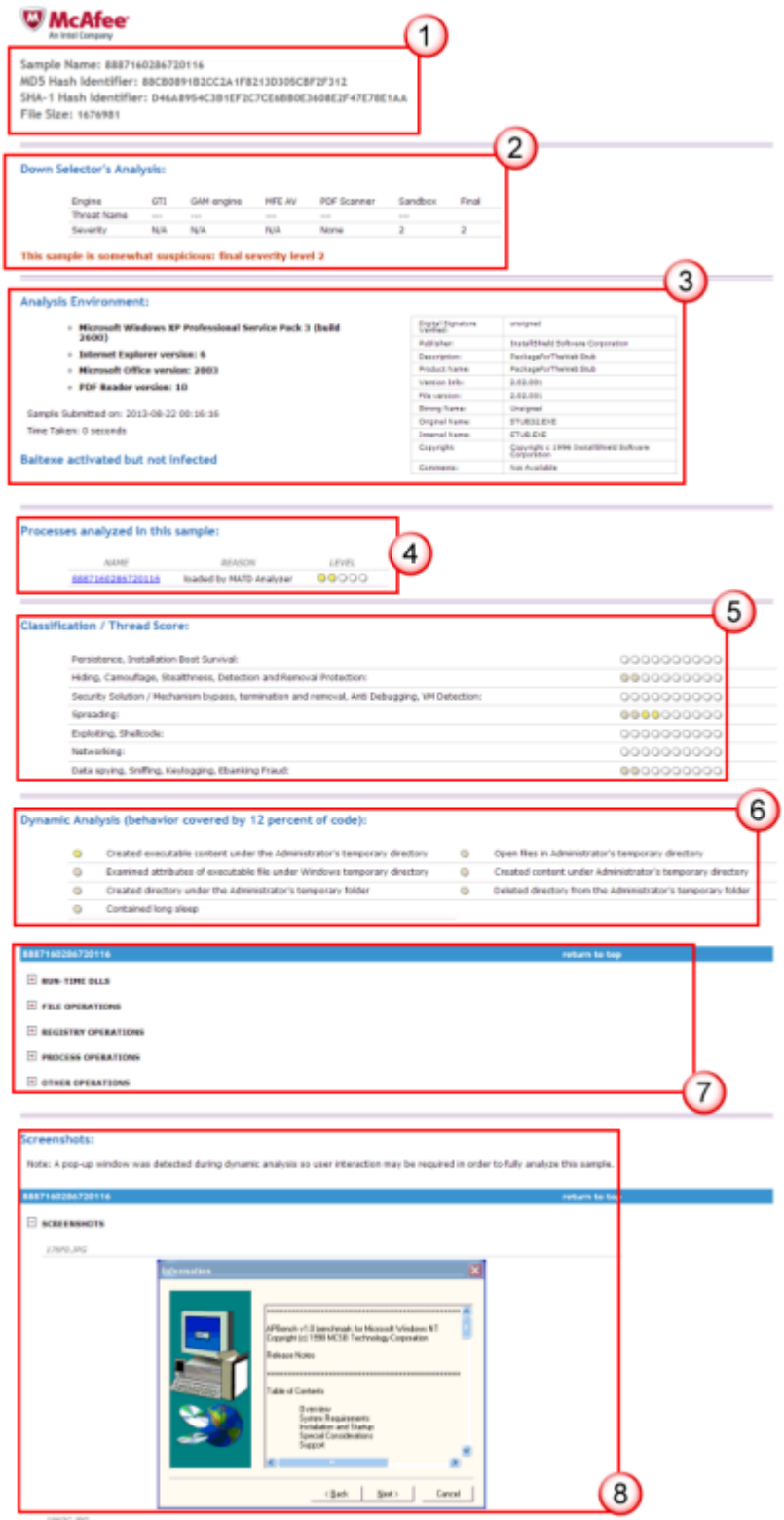

McAfee
An Intel Company
1
Sample Name: 888716028672011 6
MD5 Hash Identifier: 88CD0891B2CC2A1F8213D305CBF2F312
SHA-1 Hash Identifier: D46A895C4C3B1EF2C7CE6BB0E3608E2F47E78E1AA
File Size: 1676981
2
Down Selector's Analysis:
Engine GTI GAM engine HFE AV PDF Scanner Sandbox Final
Threat Name --- --- --- --- --- ---
Severity N/A N/A N/A None 2 2
This sample is somewhat suspicious: final severity level 2
3
Analysis Environment:
Microsoft Windows XP Professional Service Pack 3 (build 2600)
Internet Explorer version: 6
Microsoft Office version: 2003
PDF Reader version: 10
Sample Submitted on: 2013-08-22 00:16:16
Time Taken: 0 seconds
Baltexe activated but not infected
Processes analyzed in this sample:
4
NAME REASON LEVEL
888716028672011 6 loaded by MATD Analyzer
5
Classification / Thread Score:
Persistence, Installation Boot Survival:
Hiding, Camouflage, Stealthness, Detection and Removal Protection:
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:
Spreading:
Exploiting, Shellcode:
Networking:
Data spying, Sniffing, Keylogging, Ebanking Fraud:
6
Dynamic Analysis (behavior covered by 12 percent of code):
Created executable content under the Administrator's temporary directory
Examined attributes of executable file under Windows temporary directory
Created directory under the Administrator's temporary folder
Contained long sleep
Open files in Administrator's temporary directory
Created content under Administrator's temporary directory
Deleted directory from the Administrator's temporary folder
888716028672011 6 return to top
RUN-TIME DLLS
FILE OPERATIONS
REGISTRY OPERATIONS
PROCESS OPERATIONS
OTHER OPERATIONS
7
Screenshots:
Note: A pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample.
888716028672011 6 return to to
SCREENSHOTS
8

Figure 7-4 Analysis Summary report

Table 7-6 Analysis Summary report sections

Item	Description
1	This section displays the details of the sample file. This includes the name, hash values, and the file size in bytes.
2	Analysis Results section on page 108. This section provides the results from the methods used for the file and the results from those methods. This section also displays the overall severity level for the file.
3	Analysis Environment section on page 108. This section includes the details of the analyzer VM, properties of the file, and so on.
4	Processes analyzed in this sample. This section lists all the files that were executed when dynamically analyzing the sample file. It also provides the reason how each file got to be executed along with their severity score. The Reason column indicates which other file or process created or opened this file. If there is only one file in the sample, the reason displayed is *loaded by MATD Analyzer*. If the sample file is a .zip file containing multiple files or if a file opens other files, the reason for the first file is *created by <file name> & loaded by MATD Analyzer.* For the subsequent files, the Reason column indicates all the files/processes that created it and all the files/processes that opened it. The Level column indicates the severity level based on dynamic analysis for each file. • ○○○○○ — indicates a severity score of 0 and a threat level of informational. This is the severity for white-listed files. • ○○○○○ — indicates a severity score of 1 and a threat level of very low. • ●●○○○ — indicates a severity score of 2 and a threat level of low. • ●●●○○ — indicates a severity score of 3 and a threat level of medium. • ●●●●○ — indicates a severity score of 4 and a threat level of high. • ●●●●● — indicates a severity score of 5 and a threat level of very high. Click a file name to navigate to the section of the report that provides the details of the file behavior. That is, when you click a file name, you are navigated to the section indicated by 7 in the preceding figure.
5	Classification / threat score section on page 109. This section provides the individual scores for the various characteristics of a typical malware.
6	Dynamic analysis section. This section displays the percentage of the file code that was executed. For example, the file might have taken an alternative path during execution due to which some part of the code was not executed at all. This section also provides a brief executive behavior summary with the corresponding severity levels. ● indicates a very low severity behavior. ● indicates a low severity behavior. ● indicates a medium severity behavior. ● indicates a high severity behavior. ● indicates a very high severity behavior.
7	Operations details section. This section provides detailed information on all the operations performed by the sample file during dynamic analysis. These operations are grouped under corresponding groups. Expand each group for the specific operations. For example, expand **Files Operations** to view the files created, files deleted, files modified, files read, directories created or opened, directories removed, and so on.

Table 7-6 Analysis Summary report sections *(continued)*

Item	Description
8	GTI URL Reputation. This provides McAfee GTI reputation and severity for the URL.
9	Network activity. This section provides the details of every network operation during dynamic analysis of the sample.
10	Screen-shots section. This section displays all the pop-up windows during dynamic analysis. By viewing these screenshots, you can determine if user intervention is required during dynamic analysis to know the actual behavior of the file. If user intervention is required, you can submit the file manually in user-interactive mode.

Analysis Results section

This is a section in the Analysis Summary report. In this section, you can view which methods reported that a sample file contains a malware.

Table 7-7 Down Selector's Analysis

Label	Description
Engine	These are the possible methods that McAfee Advanced Threat Defense uses to analyze a file. • GTI File Reputation: Indicates McAfee GTI that is on the cloud. • Gateway Anti_Malware: Indicates McAfee Gateway Anti-Malware engine. • Anti-Malware: Indicates McAfee Anti-Malware Engine. • Sandbox: Indicates that the file was executed in an analyzer VM. Refer to the Analysis Environment section within the report to know the details of that VM.
Threat Name	Indicates the name for known malware in McAfee GTI, McAfee Gateway Anti-Malware engine, and McAfee Anti-Malware Engine.
Severity	Indicates the severity score from various methods. The highest severity score by a particular method is used to assign the final severity level for the sample.

Analysis Environment section

This is a section in the Analysis Summary report. You can find the following details in this section:

- Details of the corresponding analyzer VM such as the operating system, browser and version, and the applications and their versions installed on the analyzer VM.

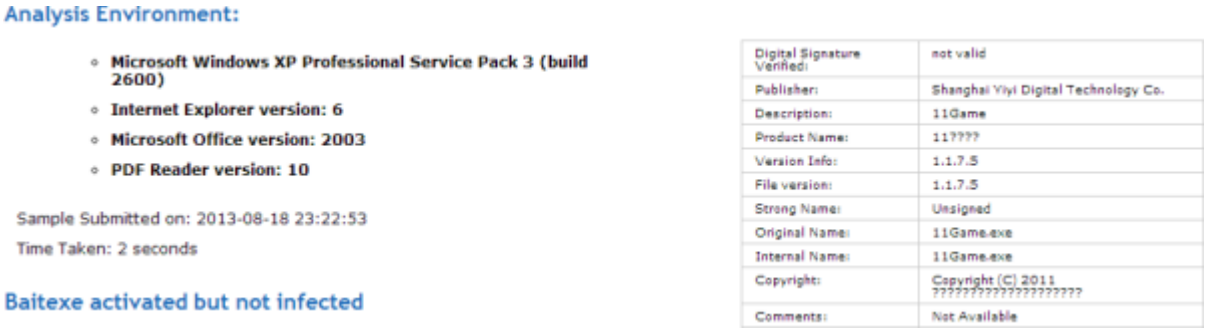

Analysis Environment:
Microsoft Windows XP Professional Service Pack 3 (build 2600)
Internet Explorer version: 6
Microsoft Office version: 2003
PDF Reader version: 10
Sample Submitted on: 2013-08-18 23:22:53
Time Taken: 2 seconds
Baitexe activated but not infected
Digital Signature Verified: not valid
Publisher: Shanghai Yiyi Digital Technology Co.
Description: 11Game
Product Name: 11????
Version Info: 1.1.7.5
File version: 1.1.7.5
Strong Name: Unsigned
Original Name: 11Game.exe
Internal Name: 11Game.exe
Copyright: Copyright (C) 2011 ??????????????????
Comments: Not Available

Figure 7-5 Analysis Environment section

- The time when the sample was submitted as per McAfee Advanced Threat Defense Appliance's clock.
- The time taken to analyze the file and generate the reports.

- On the right-hand side, a table provides the properties of the file. This includes information such as:
  - Signed or unsigned for the digital signature of the file.
  - Publisher's name if available.
  - Version details
  - Original name of the file so that you can search other sources such as the web.
- *Baitexe* process infected or not. At the end of each analysis McAfee Advanced Threat Defense creates an additional bait process called Baitexe. This Baitexe program calls two APIs (beep and sleep) only continuously. If this Baitexe process is infected by the previously executed sample, the behavior of Baitexe is different. In this case, a message *Baitexe activated and infected* is displayed. If the Baitexe process is not infected at all, the message *Baitexe activated but not infected* is displayed.

Classification / threat score section

This is a section in the Analysis Summary report, which provides the severity scores for various characteristics of a typical malware.

Table 7-8 Classification / threat score section

Label	Description
Persistence, Installation Boot Survival	Some malware have the capability to remain on the infected host. This is referred to as persistence. Installation boot survival refers to the capability of the malware to sustain even after a restart.
Hiding, Camouflage, Stealthness, Detection and Removal Protection	This refers to the capability of the malware to evade detection and removal.
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	This refers to the capability of the malware to bypass or mislead detecting methods and engines. Some malware has anti-disassembly code, which can confuse or delay malware analysis. Some malware attempt to determine if they are being executed in a sandbox. If true, they might take a different execution path. This score indicates the presence of such code in the malware.
Spreading	Indicates the capability of the malware to spread across the network.
Exploiting, Shellcode	Indicates the presence of shellcode that can exploit a running program.
Networking	Indicates the network-related behavior of the malware during dynamic analysis. For example, the malware might have triggered DNS queries or created sockets. If there is a severity score provided for this characteristic, correlate with the Network Operations details for the files in the sample.
Data spying, Sniffing, Keylogging, Ebanking Fraud	Indicates if the malware is capable of any such behaviors.

Operations details section

This section provides the details of every operation performed by a file during dynamic analysis. Separate sections are provided for every file that was executed as part of the sample.

- Run-time DLLs: Lists all the DLLs and their paths that were called by a file in runtime.
- File operations: Lists file operation activities like creation, open, query, modification, copy, move, deletion, and directory creation/deletion operations. This section also lists the file attributes and the MD5 hash value for the files.
- Registry operations: Provides the details of Windows registry operation activities like creation/open, deletion, modification, and query on registry sub-key and key entry.

- Process operations: Details the process operation activities such as new process creation, termination, new service creation, and code injection into other processes.
- Networking operations: Details networking operations such as DNS queries, TCP socket activities, and HTTP file download.
- Other operations: Provides details of operations not belonging to these categories. Examples are mutex signally objects, getting the system metric and configuration data of the analyzer VM.

Dropped files report

You can download a .zip file containing all the files that the sample created or touched during dynamic analysis. You can download these files using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click and select **Dropped Files**. Download the dropfiles.zip file, which contains the files that the sample created in the sandbox. To use this option, you must have enabled the **Dropped Files** option in the corresponding analyzer profile.
- After you click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same dropfiles.zip inside the AnalysisLog folder. The Complete Results contains the dropfiles.zip regardless of whether you have enabled **Dropped Files** option in the corresponding analyzer profile.

Disassembly Results

The Disassembly Results report provides the disassembly output listing for Portable Executable (PE) files. This report is generated based on the sample file after the unpacking process has completed. It provides detail information about the malware file such as, the PE header information.

The Disassembly Results report includes the following information:

- Date and time of the creation of the sample file
- File PE and Optional Header information
- Different section headers information
- The Intel disassembly listing

You can view the Disassembly Results report in the McAfee Advanced Threat Defense web application or download it as a file to your client computer. The contents of the report are the same in both the methods.

- To view the Disassembly Results report in the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Results**. In the **Analysis Results** page, click and select **Disassembly Results**. To use this option, you must have enabled the **Disassembly Results** option in the corresponding analyzer profile.
- To download the report as a file, click in the **Analysis Results** page and select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains a file named as <file name>_detail.asm in the AnalysisLog folder. The Zip Report contains this .asm file regardless of whether you have enabled **Disassembly Results** option in the corresponding analyzer profile.

The Disassembly Results report provides the assembler instructions along with any static standard library call names like printf and Windows system DLL API call names embedded in the listing. If the global variables such as string text are referenced in the code, these string texts are also listed.

Table 7-9 A section of a sample Disassembly Results report

Column 1	Column 2	Column 3
:00401010	e8 1f2c0000	call 00403c34 ;;call URLDownloadToFileA

The virtual address of the instruction is shown in column 1, the binary instruction in column 2, and the assembly instruction with comments is in column 3. In the preceding example the call 00403c34 instruction at memory location of 00401010 is making a functional call at 0x403c34 memory location, which is determined to be system DLL API function call determined to be URLDownloadToFileA(). The comment shown with the ;; in this listing provides the library function name.

Logic Path Graph

This report is a graphical representation of cross-reference of function calls discovered during dynamic analysis. This report enables you to view the subroutines in the analyzed file that were executed during the dynamic analysis as well as the ones that were potentially not executed. These non-executed functions could be a potential time-bomb waiting to trigger under the right conditions.

The Logic Path Graph report is available as a Graph Modeling Language (GML) file. This file is an ASCII plain text format, which contains a graphical representation of the logic execution path of the sample in the GML (Graph Modeling Language) format. You cannot directly view this file in the McAfee Advanced Threat Defense web application, but download it to your client computer. Then you must use a graphical layout editor, like yWorks yEd Graph Editor, that supports GML format. You can use such an editor to display the cross-reference of all functions using this file as an input.

You can download the Logic Path Graph file using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click and select **Logic Path Graph**. Then download the <file name>_logicpath.gml file. To use this option, you must have enabled the **Logic Path Graph** option in the corresponding analyzer profile.
- After you click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same <file name>_logicpath.gml file in the AnalysisLog folder. The Zip Report contains the <file name>_logicpath.gml file regardless of whether you have enabled **Logic Path Graph** option in the corresponding analyzer profile.

This section uses yWorks yEd Graph Editor to explain how to use the Logic Path Graph GML file. In the yEd Graph Editor, you must first set the Routing Style. You need to do this only once, and this setting is saved for further use.

1 In the yEd Graph Editor, select **Layout** | **Hierarchical.**

2 In the **Incremental Hierarchic Layout** dialog, select the **Edges** tab and select **Polyline** from the **Routing Style** drop-down list.

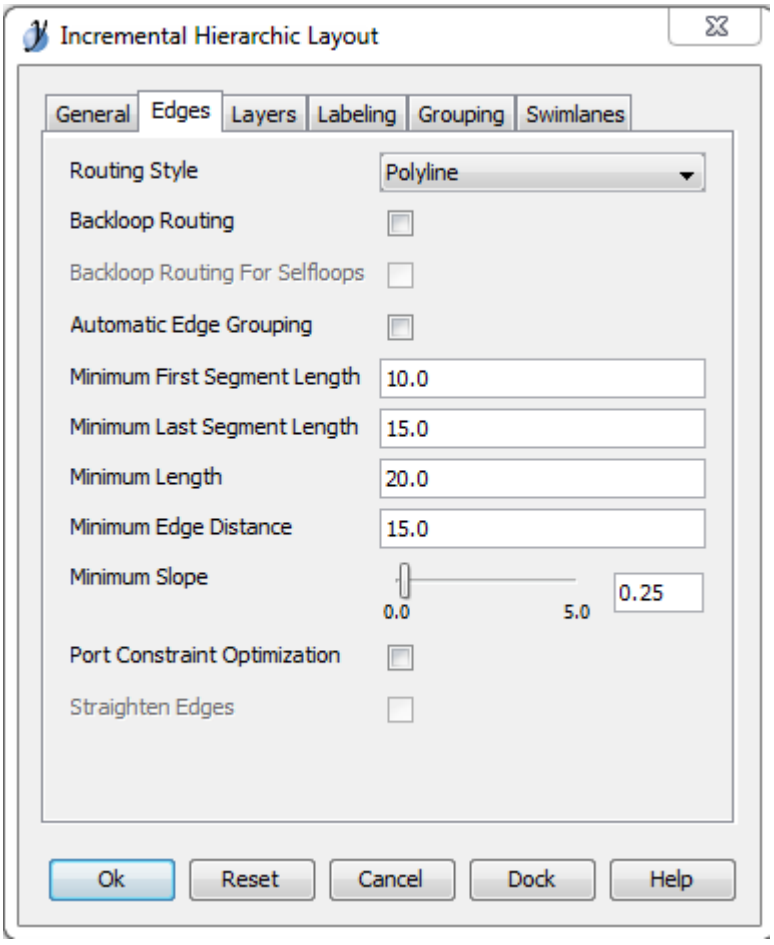


Figure 7-6 Configuring Routing Style in yEd Graph Editor

3 Click **Ok.**

When you open the <file name>_logicpath.gml file in yEd Graph Editor, initially you might see many rectangle boxes overlapping each other or a single rectangle box as shown in the following example.

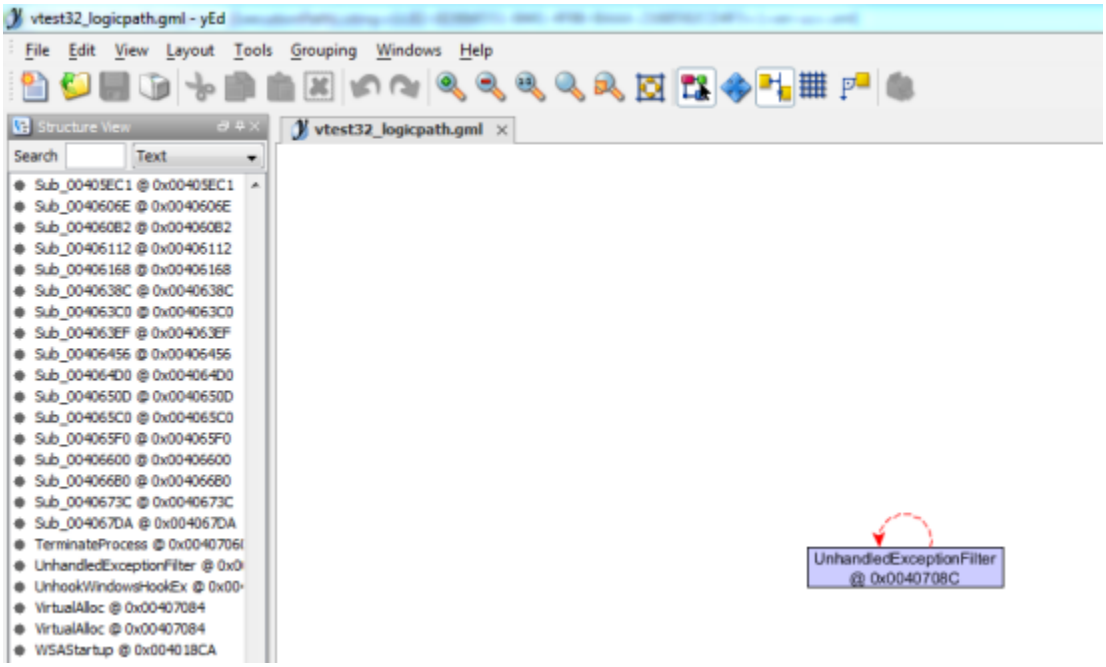


Figure 7-7 Open <file name>_logicpath.gml file

In the yEd Graph Editor select **Layout** | **Hierarchical.**

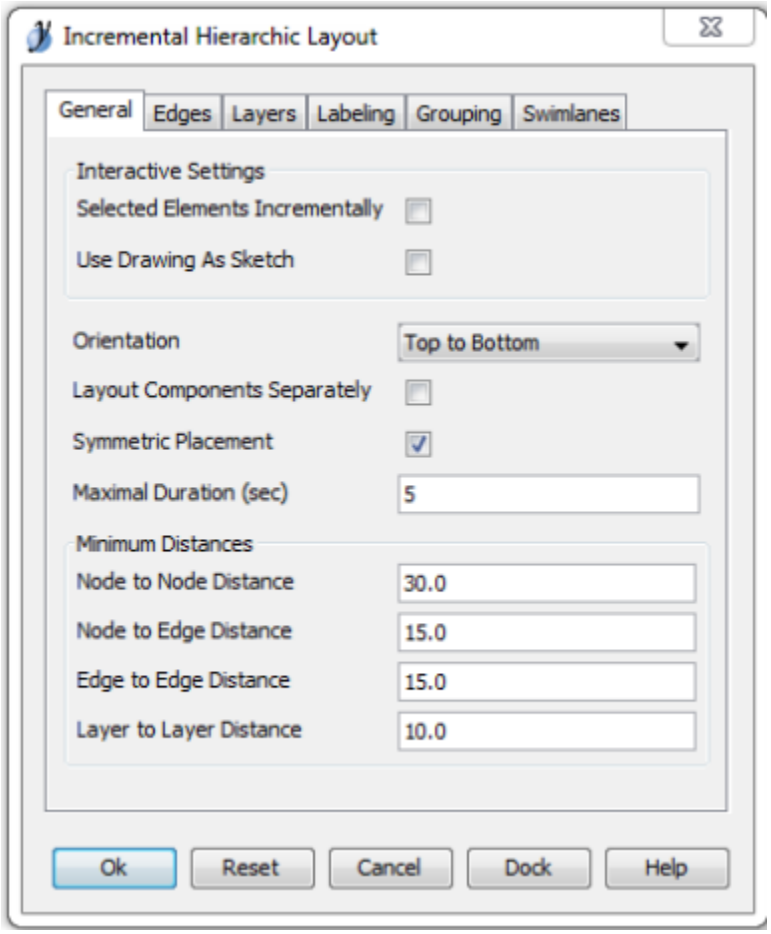


Figure 7-8 Incremental Hierarchic Layout dialog

In the **Incremental Hierarchic Layout** dialog, click **Ok** without changing any of the default settings. The following example shows the complete layout of the relationship of all subroutines detected during static disassembly processed.

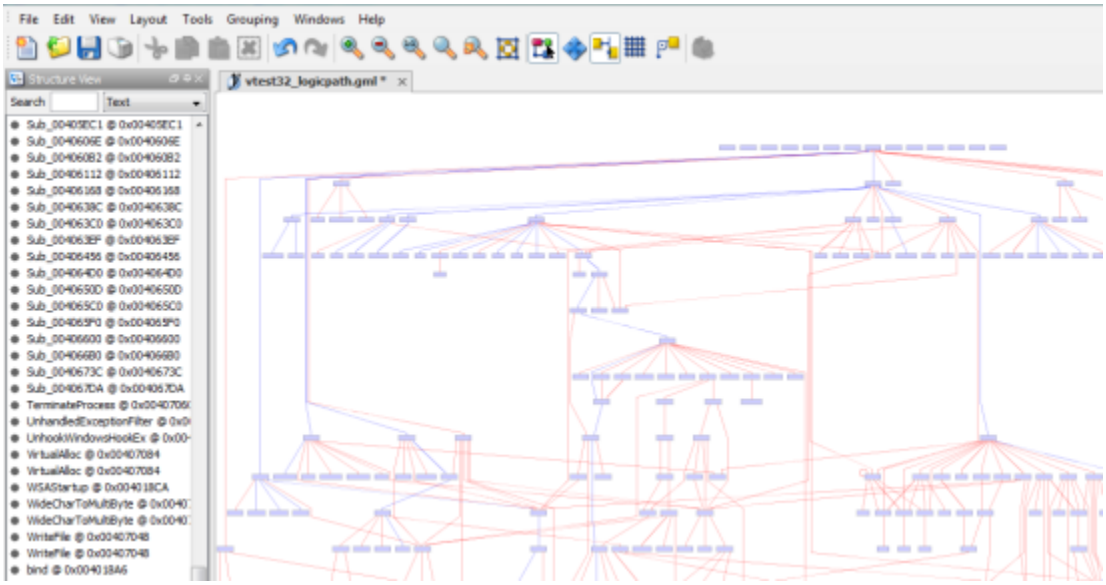


Figure 7-9 Layout of the subroutines relationships

The graph depicts an overview of the complexity of the sample as seen by the cross-reference of function calls. The following shows more detail on the function names and their addresses as seen by zooming in.

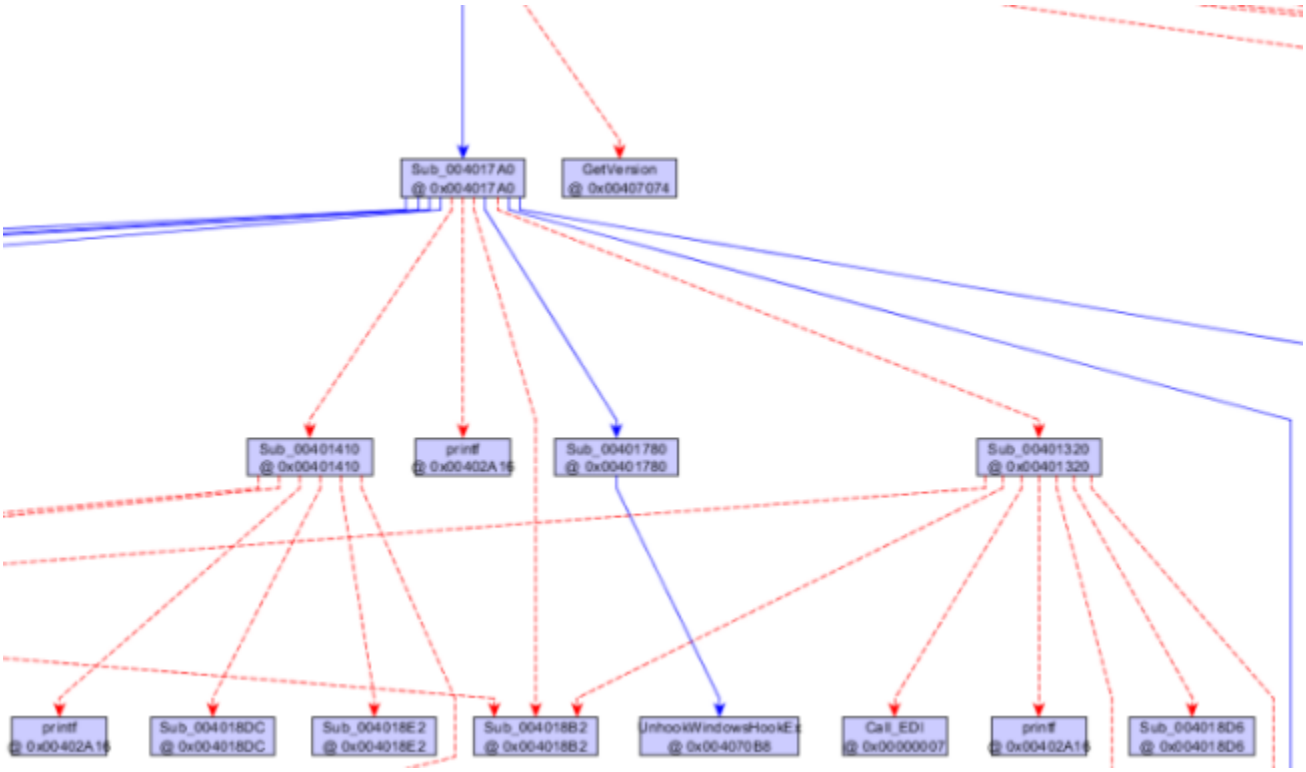


Figure 7-10 Zoom in on the layout

Two colors are used to indicate the executed path. The red dash lines show the non-executed path, and the blue solid lines show the executed path.

According to the preceding control graph, the subroutine (Sub_004017A0) at virtual address 0x004017A0 was executed and is shown with a blue solid line pointing to the Sub_004017A0 box. However, the subroutine (GetVersion]) was not called potentially as there is a red dash line pointing to it.

The Sub_004017A0 subroutine is making 11 calls as there are 11 lines coming out of this box. Seven of these 11 calls were executed during dynamic analysis. One of them is calling Sub_00401780 as there is a blue solid line pointing from Sub_004017A0 to Sub_00401780. Calls to Sub_00401410, printf, Sub_00401882, and Sub_00401320 were not executed and shown with red dashed line pointing at them.

The Sub_00401780 subroutine is making only one unique call as there is only one line coming out from this box. This call was executed during dynamic analysis.

User API Log

The User API Logs are contained in various files.

- The .log file contains the Windows user-level DLL API calls made directly by the analyzed file during dynamic analysis. To view this file in the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Results**. Then click and select **User API Log**. Alternatively, click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same information in the <sample name>.log file in the AnalysisLog folder. The content of the .log file includes the following:
  - A record of all systems DLL API calling sequence.
  - An address which indicates the approximate calling address where the DLL API call was made.
  - Optional input and output parameters, and return code for key systems DLL API calls.
- The following are the other files containing the dynamic execution logs. All these files are contained in the <sample name>.zip file.
  - <sample name>ntv.txt file. This file contains the Windows Zw version of native system services API calling sequence during the dynamic analysis. The API name typically starts with Zw as in ZwCreateFile.
  - log.zip
  - dump.zip
  - dropfiles.zip
  - networkdrive.zip

Download the complete results .zip file

McAfee Advanced Threat Defense produces detailed analysis for each submitted sample. All the available reports for an analyzed sample are available in a .zip file, which you can download from the McAfee Advanced Threat Defense web application.

Task

1 Select **Analysis** | **Analysis Results**.

2 In the **Analysis Results** page, click and select **Complete Results** .

Download the <sample_name>.zip file to the location you want. This .zip file contains the reports for each analysis. The files in this .zip file are created and stored with a standard naming

convention. Consider that the sample submitted is vtest32.exe. Then the .zip file contains the following results:

- vtest32_summary.html (.json, .txt, .xml) — This is the same as the Analysis Summary report. There are four file formats for the same summary report in the .zip file. The html and txt files are mainly for end users to review the analysis report. The .json and .xml files provide well-known malware behavior tags for high-level programming script to extract key information.
- vtest32.log — This file captures the Windows user-level DLL API calling activities during dynamic analysis. You must thoroughly examine this file to understand the complete API calling sequence as well as the input and output parameters. This is the same as the User API Log report.
- vtest32ntv.txt — This file captures the Windows native services API calling activities during dynamic analysis.
- vtest32.txt — This file shows the PE header information of the submitted sample.
- vtest32_detail.asm — This is the same as the Disassembly Results report. This file contains reverse-engineering disassembly listing of the sample after it has been unpacked or decrypted.
- vtest32_logicpath.gml — This file is the graphical representation of cross-reference of function calls discovered during dynamic analysis. This is the same as the Logic Path Graph report.
- log.zip —This file contains all the run-time log files for all processes affected by the sample during the dynamic analysis. If the sample generates any console output text, the output text message is captured in the ConsoleOutput.log file zipped up in the log.zip file. Use any regular unzip utility to see the content of all files inside this log.zip file.
- dump.zip — This file contains the memory dump (dump.bin) of binary code of the sample during dynamic analysis. This file is password protected. The password is *virus*.
- dropfiles.zip — This is the same as the Dropped Files report in the **Analysis Results** page. The dropfiles.zip file contains all files created or touched by the sample during the dynamic analysis. It is also password protected. The password is *virus*.

McAfee Advanced Threat Defense does not provide you access to the original sample files that it analyzed. If Network Security Platform is integrated, you can use the **Save File** option in the Advanced Malware policy to archive samples. However, note that the Sensor's simultaneous file scan capacity is reduced if the **Save File** option is enabled. See the latest *Network Security Platform IPS Administration Guide* for the details.

Working with the McAfee Advanced Threat Defense Dashboard

When you access McAfee Advanced Threat Defense from a client browser, the McAfee Advanced Threat Defense Dashboard is displayed. You can view the following monitors on the McAfee Advanced Threat Defense Dashboard:

- VM Creation Status — Shows the status for analyzer VMs that being created.
- File Counters — Provides a status of files being analyzed.
- Files analyzed by File Type — Provides a view of file types being analyzed.
- Top Malware by File Name — Lists the most severe malware files in your network by file name.
- Analyzer Profile Usage — Provides the details of the analyzer profiles being used.

- System Health — Provides the system health details of the McAfee Advanced Threat Defense Appliance.
- System Information — Provides the version numbers for the software components of McAfee Advanced Threat Defense Appliance.

Task

1 Click **Dashboard** to view the monitors.

2 Specify the criteria for the data to be displayed in the monitors.

a Specify the time period for the information to be displayed in the monitors.

For example, you can select to view the information for the past one hour. By default, data for the past 14 days is shown. This field does not affect the System Health and System Information monitors.

b To refresh the monitors now, click .

c Click to edit the dashboard settings.

Table 7-10 Dashboard settings

Option	Definition
Monitors	Select the monitors that you want to see on the Dashboard.
Automatic Refresh	Set the frequency at which the Dashboard should automatically refresh itself. If you want to refresh the dashboard only manually, select **Disabled**. When required to refresh the Dashboard, click . This enables you to view the snapshot of the Dashboard at a specific point in time.
Layout	Specify the number of columns into which you want to organize the Dashboard.
OK	Click to save and apply the Dashboard settings.
Cancel	Click to retain the last saved settings.

3 Optionally, set the display settings for each monitor.

- To collapse a monitor, click
- To hide a monitor, click
- To change the display format of a monitor, click

Malware analysis monitors

The following are the monitors related to malware analysis.

File Counters

This monitor shows the analysis status for files submitted during the specified time period. For example, if you set the time period for the data in the dashboard as last 5 minutes, this monitor shows the count of files in completed, analyzing, and waiting statuses since the last 5 minutes. If you view this monitor in the stacked bar chart format, it also displays the severity level for the files.

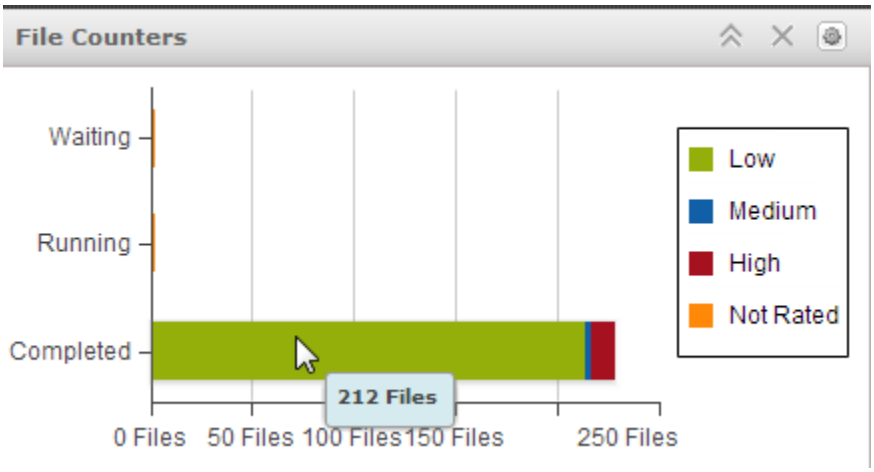


Figure 7-11 File Counters monitor

- The confidence levels are indicated using various colors.
- To hide the files for a particular confidence level, click the corresponding confidence level in the legend. For example, if you want to focus on only the high severity files, click **Low** and **Medium** in the legend. Now the chart shows only the high-severity malware that is in the waiting, running, and completed statuses. Click again on **Low** and **Medium** to view the combined chart.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

Files analyzed by File Type

This monitor shows the count of files analyzed against their type. In the tabular format, it shows the percentage for each type. In the chart, it also shows the count of infected and non-infected files.

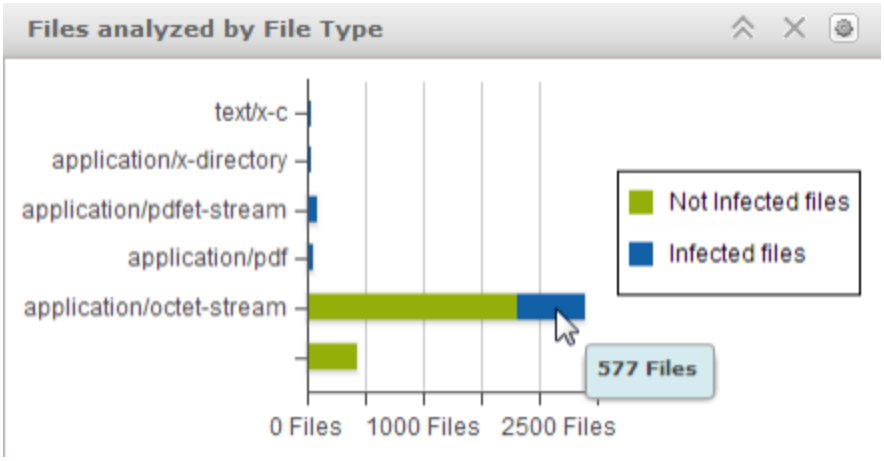


Figure 7-12 Files analyzed by File Type monitor

- The infected and not infected file counts are indicated using different colors.
- To hide the infected or not infected files, click the corresponding confidence level in the legend.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

Analyzer Profile Usage

This monitor shows the number of times each analyzer profile has been used for analyzing files.

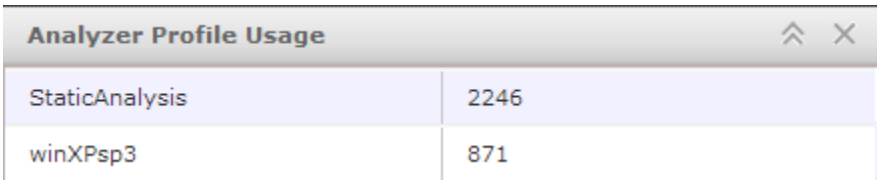


Figure 7-13 Analyzer Profile Usage monitor

Top malware by file name

In this monitor, you can view the names of the malicious files detected in your network with the most severe ones listed on top. This information might enable further research such as finding more information about these files on the web.

- The listed malware files are sorted based on their severity score in the descending order. This score is displayed in the second column. The following are the severity scores:
  - 5 — Very high severity
  - 4 — High severity
  - 3 — Medium severity
  - 2 — Low severity
  - 1 — Very low severity
  - 0 — Informational severity (white-listed files)
- The first column displays the file names. Files of the same severity are sorted in the alphabetical order.

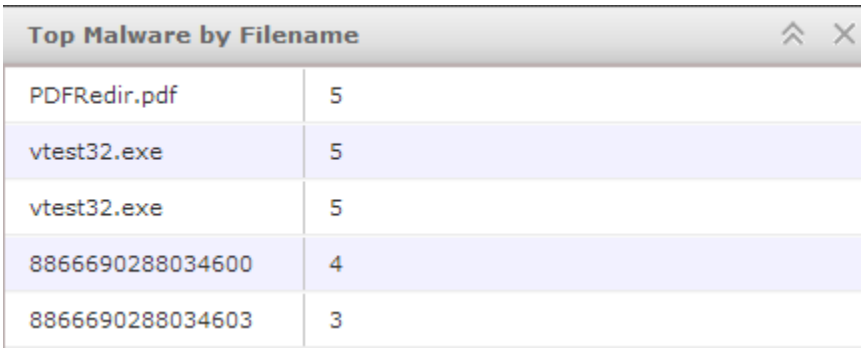


Figure 7-14 Top Malware by File Name monitor

VM Creation Status monitor

This monitor displays the status of the analyzer VMs created for the specified time period in the dashboard. For example, if you specified *Last 12 hours*, this monitor shows the status of analyzer VMs that were created in the last 12 hours.

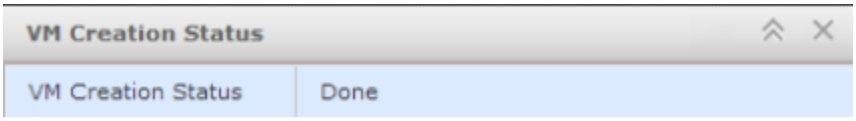


Figure 7-15 VM Creation Status monitor

McAfee Advanced Threat Defense performance monitors

The following are the monitors related to McAfee Advanced Threat Defense Appliance performance.

System Health

This monitor displays the health of the McAfee Advanced Threat Defense Appliance in a table.

- System Health — Indicates whether the system health is in good state.
- Uptime — The number of hours the Appliance has been running continuously.
- Processor Load — The percentage of the processor's capacity in use currently.
- Memory — The percentage of the Appliance's memory in use currently.
- Data Disk Space — The Appliance's disk capacity (in terabyte).
- Data Disk Available — Disk space currently available (in terabyte).

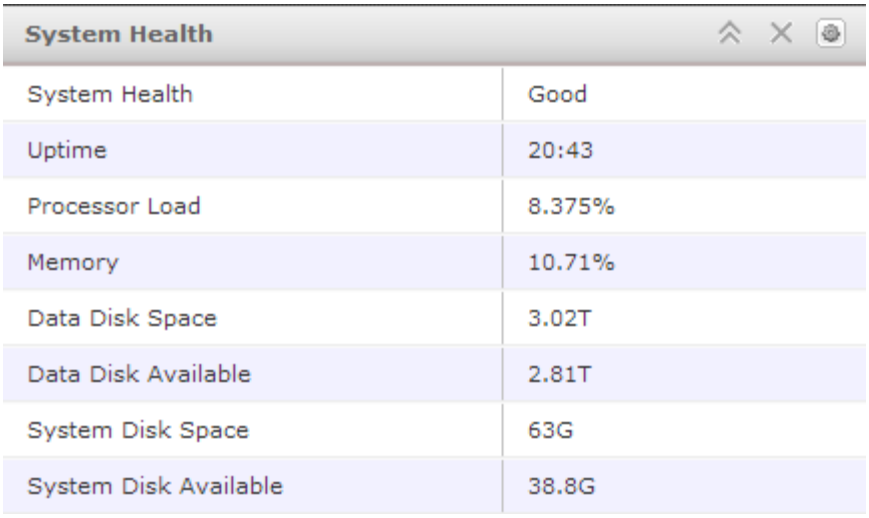


Figure 7-16 System Health monitor

- System Disk Space —
- System Disk Available —

System Information

This monitor shows the version numbers of the software components related to McAfee Advanced Threat Defense.

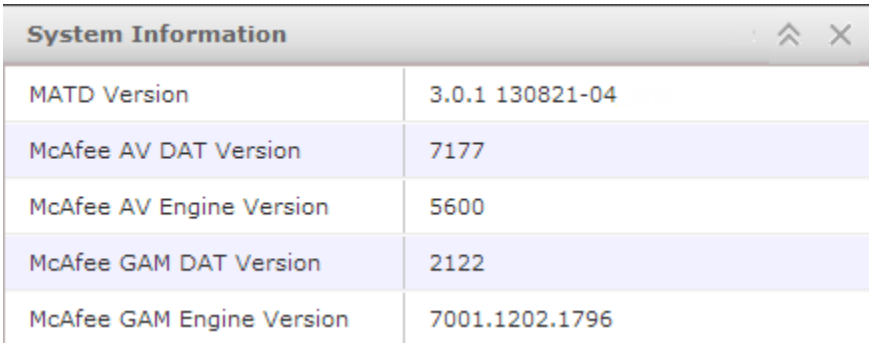


Figure 7-17 System Information monitor

8 CLI commands for McAfee Advanced Threat Defense

The McAfee Advanced Threat Defense Appliance supports command-line interface (CLI) commands for tasks such as network configuration, restarting the Appliance, and resetting the Appliance to factory defaults.

Contents

- *Issue of CLI commands*
- *CLI syntax*
- *Log on to the CLI*
- *Meaning of "?"*
- *Managing the disks of McAfee Advanced Threat Defense Appliance*
- *List of CLI commands*

Issue of CLI commands

You can issue CLI commands locally, from the McAfee Advanced Threat Defense Appliance console, or remotely through SSH.

How to issue a command through the console

For information on how to set up the console for a McAfee Advanced Threat Defense Appliance, see Configure network information for McAfee Advanced Threat Defense Appliance on page 28.

When the documentation indicates that you must perform an operation "on the Appliance," it signifies that you must perform the operation from the command line of a console host connecting to the McAfee Advanced Threat Defense Appliance. For example, when you first configure the network details for a McAfee Advanced Threat Defense Appliance, you must do so from the console.

When you are successfully connected to the McAfee Advanced Threat Defense Appliance, you will see the login prompt.

Issuing a command through SSH

You can administer a McAfee Advanced Threat Defense Appliance remotely from a command prompt over ssh.

Only 5 SSHD CLI sessions can be open concurrently on a McAfee Advanced Threat Defense Appliance.

Logging on to the McAfee Advanced Threat Defense Appliance using an SSH client

Task

1 Open an SSH client session.

2 Enter the IPv4 address of the McAfee Advanced Threat Defense Appliance and enter 2222 as the SSH port number.

3 At the logon prompt, enter the default user name atdadmin and password atdadmin.

The number of logon attempts to the McAfee Advanced Threat Defense Appliance from a client, on a single connection, is set to 3, after which the connection is closed.

The number of logon attempts to the McAfee Advanced Threat Defense Appliance can differ based on the ssh client that you are using. You can get three logon attempts with certain clients (for example, Putty release 0.54, Putty release 0.56) or you can get four logon attempts with other clients (for example, Putty release 0.58, Linux ssh clients).

Auto-complete

The CLI provides an auto-complete feature. To auto-complete a command, press Tab after typing a few characters of a valid command and then press Enter. For example, typing pas and pressing Tab would result in the CLI auto-completing the entry with the command passwd.

If the partially entered text matches multiple options, the CLI displays all available matching commands.

CLI syntax

You issue commands at the command prompt as shown.

<command> <value>

- Values that you must enter are enclosed in angle brackets (< >).
- Optional keywords or values are enclosed in square brackets ([ ]).
- Options are shown separated by a line (|).
- Variables are indicated by *italics*.

Do not type the < or [ ] symbols.

Mandatory commands

There are certain commands that must be executed on the McAfee Advanced Threat Defense Appliance before it is fully operational. The remaining commands in this chapter are optional and will assume default values for their parameters unless they are executed with other specific parameter values.

These are the required commands:

- set appliance name
- set appliance ip

- set appliance gateway is also required if any of the following are true:
  - If the McAfee Advanced Threat Defense Appliance is on a different network than the McAfee products you plan to integrate
  - If you plan to access McAfee Advanced Threat Defense from a different network either using an SSH client or a browser for accessing the McAfee Advanced Threat Defense Web Application

Log on to the CLI

Before you can enter CLI commands, you must first log on to the McAfee Advanced Threat Defense Appliance with a valid user name (default user name is atdadmin) and password (default is atdadmin). To log off, type exit.

McAfee strongly recommends you change this password using the passwd command within your first interaction with the McAfee Advanced Threat Defense Appliance.

Meaning of "?"

? displays the possible command strings that you can enter.

Syntax

?

If you use ? in conjunction with another command, it shows the next word you can type. If you execute the ? command in conjunction with the set command, for example, a list of all options available with the set command is displayed.

Managing the disks of McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliance has two disks referred to as disk-A and disk-B. Disk-A is the active disk and disk-B is the backup disk. Even if disk-A is not booted, it is referred as the active disk. Similarly, even if disk-B is the booted disk, it is referred as the backup disk. By default, both these disks contain the pre-installed software version. Subsequently, you can upgrade the software on the active disk, that is disk-A, and use disk-B to back up a stable version that you can always revert to.

Use the show command to view the software version stored in the active and backup disks.

Table 8-1 CLI commands for managing the disks

Command	Description
copyto backup	Copies the software version on the active disk to the backup disk. For example, if you find the current active software version to be stable, you can back it up to the backup disk. This command works only if the Appliance had been booted from the active disk.
copyto active	Copies the software version from the backup disk to the active disk. However, you must restart the McAfee Advanced Threat Defense Appliance for it to load this new image from the active disk. This command works only if the Appliance had been booted from the backup disk.
reboot backup	Reboots the Appliance with the software version on the backup disk.
reboot active	Reboots the Appliance with the software version on the active disk.

List of CLI commands

This section lists McAfee Advanced Threat Defense CLI commands in the alphabetical order.

Blacklist

Use the following commands to manage the blacklist of McAfee Advanced Threat Defense.

Syntax:

- To add an MD5 to the blacklist, use blacklist add <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to add to the blacklist.
<score>	The malware severity score. A valid value is from 3 to 5.
<file_name>	The file name for the MD5.
<malware_name>	The malware name for the MD5.
<Eng-ID>	The numerical ID for the corresponding engine.
<OS-ID>	The numerical ID of the operating system that was used to dynamically analyze the malware.

Example: blacklist add 254A40A56A6E28636E1465AF7C42B71F 3 ExampleFileName ExampleMalwareName 3 3

- To delete an MD5 from the blacklist, use blacklist delete <md5>

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to delete from the blacklist.

Example: blacklist delete 254A40A56A6E28636E1465AF7C42B71F

- To check if an MD5 is present in the blacklist, use blacklist query <md5>

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to query if it is present in the blacklist.

Example: blacklist query 254A40A56A6E28636E1465AF7C42B71F

If the MD5 is present, the details such as the engine ID, malware severity score, and so on, are displayed.

- To update the details for an entry in the blacklist, use blacklist update <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to update. This value must exist in the blacklist for you to update the record.
<score>	The new malware severity score that you want to change to. A valid value is from 3 to 5.
<file_name>	The new file name for the MD5.
<malware_name>	The new malware name for the MD5.
<Eng-ID>	The new engine ID that you want to change to.
<OS-ID>	The new value for the operating system that was used to dynamically analyze the malware.

Example: blacklist update 254A40A56A6E28636E1465AF7C42B71F 4 ExampleFileName ExampleMalwareName 3 4

clearstats

Resets all the McAfee Advanced Threat Defense statistics to zero.

Syntax: clearstats

This command has no parameters.

createDefaultVms

Use this command to create default analyzer VMs.

Syntax: createDefaultVms

This command has no parameters.

deleteblacklist

Use this command to remove all the entries from McAfee Advanced Threat Defense blacklist.

Syntax: deleteblacklist

This command has no parameters.

deletesamplereport

Deletes all the analysis reports for a file.

Syntax: deletesamplereport <md5>

Parameter	Description
<md5>	The MD5 value of the file for which you want to delete all the reports in McAfee Advanced Threat Defense.

Example: deletesamplereport c0850299723819570b793f6e81ce0495

diskcleanup

Use this command to delete some of the older analysis reports if the disk space of McAfee Advanced Threat Defense is low.

Syntax: diskcleanup

This command has no parameters.

Exit

Exits the CLI.

This command has no parameters.

Syntax:

exit

factorydefaults

Wipes all settings, certificates, and signatures, from the McAfee Advanced Threat Defense Appliance, clearing it to blank settings. This command does not appear when you type ? nor does the auto-complete function applies to this command. You must type the command in full to execute it.

This command has no parameters.

You are warned that the operation will clear the McAfee Advanced Threat Defense Appliance and you must confirm the action. The warning occurs since the McAfee Advanced Threat Defense Appliance returns to its clean, preconfigured state, thus losing all current configuration settings.

Syntax:

factorydefaults

gti_restart

Restarts the McAfee GTI engine of McAfee Advanced Threat Defense.

Syntax: gti_restart

This command has no parameters.

help

Provides a description of the interactive help system.

This command has no parameters.

Syntax:

help

list

Lists all the CLI commands available to users.

Syntax: list

This command has no parameters.

nslookup

Displays nslookup query result for a given domain name. You can use this to verify if McAfee Advanced Threat Defense is able to perform nslookup queries correctly.

Syntax: nslookup <WORD>

Parameter	Description
<WORD>	The domain name for which you want to query for nslookup.

Example: nslookup mcafee.com

passwd

Changes the password of the CLI user (atdadmin). A password must be between 8 and 25 characters in length and can consist of any alphanumeric character or symbol.

You are asked to enter the current password before changing to a new password.

Syntax:

passwd

ping

Pings a network host. You can specify an IPv4 address.

Syntax:

ping <A.B.C.D>

Parameter	Description
<A.B.C.D>	denotes the 32-bit IP address written as four eight-bit numbers separated by periods. Each number (A, B, C or D) is an eight-bit number between 0–255.

quit

Exits the CLI.

This command has no parameters.

Syntax:

quit

reboot

Reboots the McAfee Advanced Threat Defense Appliance with the image in the current disk. You must confirm that you want to reboot.

Syntax:

reboot

Parameter	Description
reboot active	Reboots the Appliance with the software version on the active disk.
reboot backup	Reboots the Appliance with the software version on the backup disk.
reboot vmcreator	Recreates the analyzer VMs configured in the McAfee Advanced Threat Defense web application, while rebooting the Appliance.

resetusertimeout

Enables users to log on to McAfee Advanced Threat Defense web application without waiting for the timer to expire.

Syntax: resetusertimeout <WORD>

Parameter	Description
<WORD>	The McAfee Advanced Threat Defense web application user name for which you want to remove the logon timer. If this action is successful, the message *Reset done!* is displayed.

Example: resetusertimeout admin

route add/delete network

CLI commands are available for adding and deleting static route to McAfee Advanced Threat Defense.

To add a port

route add network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>

Example: route add network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1

To delete a port

route delete network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>

Example: route delete network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1

set appliance ip

Specifies the McAfee Advanced Threat Defense Appliance IPv4 address and subnet mask. Changing the IP address requires a restart for the changes to take effect. See the reboot command for instructions on how to reboot the McAfee Advanced Threat Defense Appliance.

Syntax:

set appliance ip <A.B.C.D E.F.G.H>

Parameter	Description
<A.B.C.D E.F.G.H>	indicates an IPv4 address followed by a netmask. The netmask strips the host ID from the IP address, leaving only the network ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address(For example, the default netmask setting for a Class C address is 255.255.255.0).

Example:

set appliance ip 192.34.2.8 255.255.0.0

set appliance gateway

Specifies IPv4 address of the gateway for the McAfee Advanced Threat Defense Appliance.

Syntax:

set appliance gateway <A.B.C.D>

Parameter	Description
<A.B.C.D>	a 32-bit address written as four eight-bit numbers separated by periods. A, B, C or D represents an eight-bit number between 0–255.

Example:

set appliance gateway 192.34.2.8

set appliance name

Sets the name of the McAfee Advanced Threat Defense Appliance. This name is used to identify the McAfee Advanced Threat Defense Appliance if you integrate it with Network Security Platform.

Syntax:

set appliance name <WORD>

Parameter	Description
<WORD>	indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

Example:

set appliance name SanJose_MATD1

set intfport

Use this command to enable or disable McAfee Advanced Threat Defense interface ports.

Syntax

set intfport <1><2><3> <enable><disable>

Example: set intfport 1 enable

set intfport auto

Sets an interface port to auto-negotiate the connection with the immediate network device.

Syntax:

set intfport <1><2><3> auto

Example:

set intfport 1 auto

set intfport ip

Sets an IP address to an interface port.

Syntax:

set intfport <1><2><3> ip A.B.C.D E.F.G.H

Example:

set intfport 1 10.10.10.10 255.255.255.0

set intfport speed duplex

Set the speed and duplex setting on the specified interface port.

Syntax:

set intfport <1><2><3> speed <10 | 100> duplex <half | full>

Parameter	Description
<1> <2> <3>	Enter an interface port ID for which you want to set the speed and duplex.
<10 | 100>	Sets the speed on the interface port. The speed value can be either 10 or 100
<half | full>	Sets the duplex setting on the interface port. Set the value "half' for half duplex and full for 'full' duplex.

Example:

set intfport 1 speed 100 duplex full

set mgmtport auto

Configures the network port to auto-negotiate the connection between the McAfee Advanced Threat Defense Appliance and the immediate network device.

This command has no parameters.

Syntax:

set mgmtport auto

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set mgmtport speed and duplex

Configures the network port to match the speed of the network device connecting to the McAfee Advanced Threat Defense Appliance and to run in full- or half-duplex mode.

Syntax:

set mgmtport <speed <10 | 100> duplex <full | half>>

Parameter	Description
<10|100>	sets the speed on the Ethernet network port. The speed value can be either 10 or 100 Mbps. To set the speed to 1000 Mbps, use the set mgmtport auto command.
<half|full>	sets the duplex setting on the Ethernet network port. Set the value half for half duplex and full for full duplex.

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set_ui_timeout

Specifies the number of minutes of inactivity that can pass before the McAfee Advanced Threat Defense web application connection times out.

Syntax:

set_ui_timeout <60 - 86400>

Parameter	Description
<60 - 86400>	You can set a timeout period from 60 to 86400 seconds.

Example: set_ui_timeout 600

Default Value: 15 minutes

setwhitelist

Use this command to configure checking of whitelist by McAfee Advanced Threat Defense. By default, it is enabled.

Syntax:

setwhitelist <enable><disable>

Example: setwhitelist enable

show

Shows all the current configuration settings on the McAfee Advanced Threat Defense Appliance.

This command has no parameters.

Syntax:

show

Information displayed by the show command includes:

[Sensor Info]

- System Name
- Date
- System Uptime
- System Type
- Serial Number
- Software Version
- Active Version
- Backup Version
- MGMT Ethernet Port

[Sensor Network Config]

- IP Address
- Netmask
- Default Gateway

show epo-stats nsp

Displays the count of requests sent to McAfee ePO, the count of responses received from McAfee ePO, and the count of requests that failed.

Syntax: show epo-stats nsp

This command has no parameters.

show history

Displays the list of CLI commands issued in this session.

Syntax: show history

This command has no parameters.

show intfport

Shows the status of the specified interface port or the management port of McAfee Advanced Threat Defense.

Syntax: show intfport <mgmt><1><2><3>

Information displayed by the show intfport command includes:

- Whether the port's administrative status is enabled or disabled.
- The port's link status.
- The speed of the port.
- Whether the port is set to half or full duplex.
- Total packets received.
- Total packets sent.
- Total CRC errors received.
- Total other errors received.
- Total CRC errors sent.
- Total other errors sent.
- IP address of the port.
- MAC address of the port.

show nsp scandetails

Shows the file scan details regarding the integrated IPS Sensors.

Syntax: show nsp scandetails <Sensor IP address>

If you do not specify the Sensor IP address, the details are displayed for all the Sensors integrated with the McAfee Advanced Threat Defense Appliance.

Information displayed by the show nsp scandetails command includes:

- The IP address of the IPS Sensor.
- Total number of packets received from the Sensor.
- Total number of packets sent to the Sensor.
- The timestamp of when the last packet was sent to and received from the Sensor.
- The encryption method used for the communication with the Sensor.
- Session handle null counts.
- Count of internal errors.
- Count of unknown commands received from the Sensor.
- File string null.
- File data null.
- Count of unknown files.
- Count of out of order packets.
- Count of MD5 mismatches between what was sent by the Sensor and what was calculated by McAfee Advanced Threat Defense.
- Count of memory allocation failures.
- File transfer timeout.
- New file count.
- Count of shared memory allocation failures.
- Count of the number of static analysis responses sent.
- Count of the number of dynamic analysis responses sent.
- Count of scan request received.
- MD5 of the last file that was streamed by the Sensor.

show route

This command is used to show routes that you configured using the route add command as well as the system IP routing table.

Syntax:

show route

The details from a sample output of the command in the following table.

Table 8-2 System IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.10.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
11.11.11.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
12.12.0.0	0.0.0.0	255.255.0.0	U	0	0	0	mgmt

Table 8-2 System IP routing table *(continued)*

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
13.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	mgmt
0.0.0.0	10.10.10.253	0.0.0.0	UG	0	0	0	mgmt

shutdown

Halts the McAfee Advanced Threat Defense Appliance so you can power it down. Then, after about a minute, you can power down the McAfee Advanced Threat Defense Appliance manually and unplug both the power supplies. McAfee Advanced Threat Defense Appliance does not power off automatically. You must confirm that you want to shut it down.

This command has no parameters.

Syntax:

shutdown

status

Shows McAfee Advanced Threat Defense system status, such as the health and the number of files submitted to various engines.

This command has no parameters.

Syntax: status

Sample output:

System Health Status : good

Sample files received count: 300

Sample files submitted count: 300

GTI Scanner files submitted count: 50

GAM Scanner files submitted count: 100

MAV Scanner files submitted count: 200

Sandbox files submitted count: 25

Sandbox files finished count: 25

Sample files finished count: 300

Sample files error count: 0

update_avdat

Updates the DAT files for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine.

This command has no parameters.

Syntax: update_avdat

watchdog

The watchdog process reboots the McAfee Advanced Threat Defense Appliance whenever an unrecoverable failure is detected.

Syntax:

watchdog <on | off | status>

Parameter	Description
<on>	Enables the watchdog.
<off>	Disables the watchdog. Use it if the Appliance reboots continuously due to repeated system failure.
<status>	Displays the status of the watchdog process.

whitelist

Use the following commands to manage the whitelist of McAfee Advanced Threat Defense.

Syntax:

- To add an MD5 to the whitelist, use whitelist add <md5>
  Example: whitelist add 254A40A56A6E68636E1465AF7C42B71F
- To delete an MD5 from the whitelist, use whitelist delete <md5>
  Example: whitelist delete 254A40A56A6E28836E1465AF7C42B71F
- To check if an MD5 is present in the whitelist, use whitelist query <md5>
  Example: whitelist query 254A40A56A6E28636E1465AF7C42B71F
- To check the status if checking the whitelist status is currently enabled, use whiteliststatus

Index

A

about this guide 7

C

CLI commands issue 123
- auto-complete 124
- console 123
- mandatory commands 124
- ssh 123

CLI logon 125
CLI syntax 124
conventions and icons used in this guide 7

D

documentation
- audience for this guide 7
- product-specific, finding 8
- typographical conventions and icons 7

M

McAfee ServicePortal, accessing 8

N

network recommendations 23
NIC ports 18

R

rule objects
- add 35, 76, 89
- delete 38, 91
- modify 37, 80, 91
- view 34, 75, 88

S

Sensor logon; ssh 124
ServicePortal, finding product documentation 8
system requirements; client 31

T

Technical Support, finding product information 8

W

Warnings 19

McAfee
An Intel Company